

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-163882

(43)Date of publication of application : 16.06.2000

(51)Int.Cl.

G11B 20/12

G06F 12/00

G06F 12/14

G06K 17/00

G06K 19/07

G06K 19/073

G06K 19/10

G09C 1/00

G09C 5/00

G11B 20/10

H04L 9/10

H04L 9/32

(21)Application number : 10-340487 (71)Applicant : MATSUSHITA ELECTRIC
IND CO LTD

(22)Date of filing : 30.11.1998 (72)Inventor : HIROTA TERUTO
KOZUKA MASAYUKI
TATEBAYASHI MAKOTO

(54) DIGITAL LITERARY PRODUCTION RECORDING MEDIUM, RECORDING
DEVICE ACCESSING SAME RECORDING MEDIUM, AND REPRODUCING
DEVICE AND DELETING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain the digital literary production recording medium which is digital literary production is recorded in optimum digital structure in terms of both security and use.

SOLUTION: Digital literary production data ciphered by using different file keys by files are recorded as files and in ciphered file key fields 211 in file entries as management information for access corresponding to the files, ciphered file keys obtained by ciphering the file keys by using media characteristic keys as a key characteristic of the recording medium are recorded.

LEGAL STATUS

[Date of request for examination] 13.09.2005

[Date of sending the examiner's
decision of rejection]

[Kind of final disposal of application withdrawal
other than the examiner's decision of

rejection or application converted
registration]

[Date of final disposal for application] 13.12.2006

[Patent number]

[Date of registration]

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against
examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] It is the digital work record medium which recorded as a file the digital work data enciphered using the 1st key and in which computer reading is possible. The management information field as a logical field which recorded the management information which corresponds to said file and includes the information about the record location of the file concerned is included. Said management information field is a digital work record medium characterized by including the field which recorded further the 1st key of encryption which enciphers said 1st key using the 2nd key.

[Claim 2] Said 2nd key is a digital work record medium according to claim 1 characterized by what is independently recorded on the field different from the 1st key of encryption.

[Claim 3] Said management information field is a digital work record medium according to claim 1 or 2 characterized by including the field which recorded the encryption existence flag which shows whether the content of the field which

recorded said 1st key of encryption is still more effective.

[Claim 4] Said management-information field is the digital work record medium characterized by to include the field which recorded the information showing said digital watermarking further including the management-information field as a logical field which is the digital work record medium which recorded as a file the digital work data with which digital watermarking was embedded, and in which computer reading is possible, and recorded the management information which corresponds to said file and includes the information about the record location of the file concerned.

[Claim 5] It is the digital work record medium according to claim 4 which said digital watermarking is the information about said digital work copy-of-data propriety, and is characterized by the information showing said digital watermarking being encryption digital watermarking which enciphers said digital watermarking using the 2nd key.

[Claim 6] It is the digital work record medium which recorded as a file what enciphered the digital work data with which digital watermarking was embedded using the 1st key and in which computer reading is possible. The management information field as a logical field which recorded the management information which corresponds to said file and includes the information about the record location of the file concerned is included. Said management information field is a digital work record medium characterized by including the field which recorded further the 1st key of encryption which enciphers said 1st key using the 2nd key, and the field which recorded what enciphered said digital watermarking using said 1st key or said 2nd key.

[Claim 7] Said management information field is a digital work record medium according to claim 6 characterized by including the field which enciphered and recorded what doubled said 1st key and said digital watermarking using said 2nd key.

[Claim 8] Said digital work record medium is a digital work record medium according to claim 4 characterized by having the active component which

performs mutual recognition further between the equipment which accesses the digital work record medium concerned.

[Claim 9] Said digital work record medium has the active component which performs mutual recognition further between the equipment which accesses the digital work record medium concerned. Said 2nd key A digital work record medium given in claims 1-3 which are the keys of a value peculiar to said digital work record medium, and are characterized by transmitting to said equipment what enciphered said 2nd key from said digital work record medium in the process of said mutual recognition, and any 1 term of 5-7.

[Claim 10] Said file is Universal. Disk It is recorded according to Format and said management information field is Universal. Disk The field which is a file entry in Format and recorded said 1st key of encryption is a digital work record medium according to claim 1 characterized by being an extended attribute field in said file entry.

[Claim 11] The field which said file was recorded according to the FAT mold format in said digital work record medium, and said management information field is a directory item in a FAT mold format of JIS-X-0605 specification, and recorded said 1st key of encryption is a digital work record medium according to claim 1 characterized by being a free space in said directory item.

[Claim 12] An authentication means to be the recording device which records as a file the digital work data enciphered after the authentication success on a record medium equipped with the active component which has an authentication function, and to perform said record medium and mutual recognition, A file record means to record on said record medium by considering said digital work enciphered using the 1st key as a file, The recording device characterized by being one logically, and including said 1st key enciphered using the 2nd key, and the information about the record location of said file in the management information field corresponding to the file concerned by 1 to 1, and recording them on said record medium.

[Claim 13] The digital work data which were equipped with the active component

which has an authentication function, and were enciphered using the 1st key are recorded as a file. and from the record medium with which what said 1st key was enciphered as using the 2nd key, and the information about the record location of the file concerned are recorded on the logical management information field An authentication means to be the regenerative apparatus which reads and decodes the enciphered digital work data concerned, and is reproduced after an authentication success, and to perform said record medium and mutual recognition, A 1st key decode means to read said 1st enciphered key which is recorded on said management information field, and to decode using said 2nd key, The regenerative apparatus characterized by having a data decode playback means to decode and reproduce using the 1st key which read the enciphered digital work data which are recorded as said file, and was decoded by said 1st key decode means.

[Claim 14] The digital work data which were equipped with the active component which has an authentication function, and were enciphered using the 1st key are recorded as a file. and from the record medium with which the deletion information which shows whether what said 1st key was enciphered as using the 2nd key, the information about the record location of the file concerned, and the file concerned are deleted is recorded on the logical management information field An authentication means to be deletion equipment which deletes the enciphered digital work data concerned logically after an authentication success, and to perform said record medium and mutual recognition, Read said 1st enciphered key which is recorded on said management information field, and said 1st key decoded and obtained using said 2nd key is enciphered with said 2nd key and the 3rd different key. the deletion equipment characterized by updating so that the purport from which it records on said location which carried out reading appearance, and a file is deleted in said deletion information in said management information field may be shown.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the access equipment to the record medium concerned, concerning the DS of the record medium for recording a digital work.

[0002]

[Description of the Prior Art] Contents, such as music which is a digital work, come to be distributed by development of a multimedia network technique through the Internet etc. in recent years, and it has become possible to touch the music in the world etc. at a house. Moreover, such a music content etc. can also be recorded on storages, such as semiconductor memory. Reading appearance of the contents, such as music recorded on record media, such as semiconductor memory, is carried out with the music regenerative apparatus of for example, a pocket mold, and they are reproduced.

[0003] By the way, when recording data on a record medium, it is collected in content, and since it is [a certain data] handling-easy and they are carried out in the unit, using the concept of a file, file which is a settlement of data, and management information for managing a file can be made into a pair, and can be recorded on a record medium. Management information is information which shows attributes and sizes, such as access propriety about a file, a file location, etc., and can perform access to a file by referring to this management information.

[0004] The digital work recorded on a record medium should be effectively protected from unjust utilization, and in order to realize safe positive contents distribution through the Internet etc., security techniques, such as encryption and digital watermarking, are used.

[0005]

[Problem(s) to be Solved by the Invention] However, although the security

technique about contents distribution was developed conventionally, the format at the time of recording contents on a record medium, i.e., somatization of the above-mentioned security technique about the DS of a record medium, is inadequate, and when recording contents as a file now, the optimal DS for attaining protection of the author of contents and a rightful claimant and easy-ization of utilization of contents is searched for.

[0006] Then, this invention is made in view of such a request, and aims at offering the digital work record medium with which the digital work was recorded by the optimal DS in the security side and the utilization side.

[0007]

[Means for Solving the Problem] The digital work record medium applied to this invention in order to solve the above-mentioned technical problem It is the digital work record medium which recorded as a file the digital work data enciphered using the 1st key and in which computer reading is possible. The management information field as a logical field which recorded the management information which corresponds to said file and includes the information about the record location of the file concerned is included. It is characterized by said management information field including the field which recorded further the 1st key of encryption which enciphers said 1st key using the 2nd key.

[0008] By the above-mentioned configuration, since the 1st key used for encryption of the content of the file is recorded on the management information field which is a logical field, it cannot be dependent on characteristic DS, such as contents which are not dependent on the physical structure of a record medium, and serve as a file content, etc., and the 1st key, i.e., a file key, can be enciphered and recorded. Moreover, the digital work record medium concerning this invention is the digital work record medium which recorded as a file the digital work data with which digital watermarking was embedded and in which computer reading is possible, and it is characterized by for said management-information field to include the field which recorded the information showing said digital watermarking further including the management-information field as a

logical field which recorded the management information which corresponds to said file and includes the information about the record location of the file concerned.

[0009] Since digital watermarking is recorded all over the management information field in a record medium by the above-mentioned configuration, the equipment which performs the copy of the file in the record medium concerned etc. does not need to extract digital watermarking from the enciphered digital work data which are a file content directly, and refer to the digital watermarking for it easily by it. Although it has the fault that the circuit magnitude of the circuit for a digital-watermarking extract is also large, its power consumption is also high, and an extract takes time amount, when it is not necessary to build in the circuit for a digital-watermarking extract, and small lightweight-ization can be attained and said digital watermarking includes the information about the copy propriety of a file, since said equipment can refer to the digital watermarking concerned easily, according to this invention, the quick copy of it etc. is attained.

[0010]

[Embodiment of the Invention] Hereafter, the DS of the digital work record medium concerning this invention is explained using a drawing.

<Gestalt 1 of operation> <DS in 1. flash memory> drawing 1 is drawing showing the logical DS of the digital work record medium (flash memory) concerning the gestalt 1 of operation of this invention.

[0011] The flash memories shown in this drawing are some IC cards (henceforth a memory card) which can record a digital work, and are flash memories with the storage capacity which is 64 megabytes [read-out / data / megabytes / writing and read-out]. In addition, a memory card is the configuration of several mm in thickness, and 2cm four-way-type extent of every direction, and has an active component with functions other than a flash memory, such as an access control of mutual recognition and a flash memory.

[0012] Various information is stored in a flash memory in a logical format similar to UDF (Universal Disk Format). namely, a part of volume structure information

101 and volume structure information -- a file entry 130, data 140 and 150, and 160 grades are stored if needed besides a copy 102, the file set descriptor 103, the file entry 110 of the root, and the directory data 120.

[0013] The volume structure information 101 is the information about the whole record medium, and includes information, such as whole capacity. The file set descriptor 103 includes information, such as a character code used for the information which shows arrangement of the file entry 110 of the root, or a file name. The file entry 110 of the root is a file entry of a root directory, and shows arrangement of the directory data 120.

[0014] The directory data 120 are the set of the file identification descriptors 121, 122, and 123 which show arrangement and the file name of a file entry. Signs that the file identification descriptor 122 includes the information which shows arrangement of a file entry 130 are shown in this drawing. A file entry 130 includes the information which shows arrangement of the data 140, 150, and 160 which constitute a file. In addition, a file entry serves as data or directory data, and a pair, and exists.

[0015] Drawing 2 is drawing showing the DS of a file entry. A file entry The DescriptorTag field 201, the ICBTag field 202, the Uid field 203, the Gid field 204, the AccessTime field 205, the ModificationTime field 206, The UniqueID field 207, the LengthOfExtendedAttributes field 208, the LengthOfAllocationDescriptors field 209, the encryption attribute field length field 210, It is a thing containing the encryption file key field 211, the encryption WM field 212, and the] field 213 and ExtendedAttributes[AllocationDescriptors[] field 214 grade. The size is 2048 bytes fundamentally. It is the part from which the encryption attribute field length field 210, the encryption file key field 211, and the encryption WM field 212 are different from UDF, and serve as the description of this invention.

[0016] The ICBTag field 202 is the field which stores the information which shows a file type and an attribute, it is the field which stores the predetermined identifier which shows that the DescriptorTag field 201 is a file entry, and the Gid field 204 is [the Uid field 203 is the field which stores the identifier of the owner of a file,

and] the field which stores the identifier of the group of a file.

[0017] The AccessTime field 205 is the field which stores the information which shows the time of day which read the file, the ModificationTime field 206 is the field which stores the information which shows the time of day which updated the file, and the UniqueID field 207 is the field which stores the identifier of a file proper.

[0018] ExtendedAttributes[] The field 213 is the field which can store two or more information which shows an extended attribute, and the

LengthOfExtendedAttributes field 208 is the field which stores the area size of the ExtendedAttributes[] field 213. The AllocationDescriptors

[Allocationdescriptors[of file entry 130 which the] field 214 is the field which stores information which shows arrangement of file, for example, is shown in drawing 1] field stores the information which shows arrangement of data 140, 150, and 160. The LengthOfAllocationDescriptors field 209 is the field which stores the area size of the Allocationdescriptors[] field 213.

[0019] The encryption file key field 211 64 bit data obtained as a result of enciphering with a DES (Data Encryption Standard) algorithm to the 56-bit file key which is a key used for the data encryption which is the content of the file (it is hereafter called an encryption file key.) It is digital watermarking (it is hereafter called WM (WaterMark).) which is 8 bytes of field to store and is contained in the data whose encryption WM field 212 is the content of the file. It is 8 bytes of field which stores what was extracted and enciphered. Here, WM shall consider as the 2 same bit data as CGMS (Copy Generation Management System) currently embedded to contents data in DVD, and shall store in the encryption WM field 212 64 bit data (henceforth Encryption WM) obtained by enciphering with a DES algorithm to the 2 bit data concerned.

[0020] In addition, 2 bit data of CGMS being copied copy freedom (Free), the prohibition (Never) on a copy, and once (One Copy) and the value which means either of the prohibitions (No More Copy) on the further copy by copy ending once are taken. Moreover, it is shown whether the encryption attribute field

length field 210 has the effective value which stored the size of the encryption file key field 211 and the encryption WM field 212, and was stored in these fields, when a value is 16, an encryption file key and Encryption WM are effective, and when a value is 0, an encryption file key and Encryption WM mean an invalid thing.

[0021] Drawing 3 is drawing showing the DS of a file identification descriptor. A file identification descriptor constitutes the directory data 120 (refer to drawing 1), and including the information indicating a file entry, as shown in drawing 3 , it consists of the FileCharacteristics field 301, the ICB field 302, and FileIdentifier field 303 grade. It is the field which stores the block address the ICB field 302 indicates arrangement of a file entry to be here, and the FileCharacteristics field 301 is the field which stores the information a file indicates it to be whether it is a deleted file or it is a directory, and the FileIdentifier field 303 is the field where the information which shows a file name or a directory name is stored.

[0022] The music content record system which records a music content by the DS mentioned above to the memory card is explained below <2. music content record system>.

<2-1. configuration> drawing 4 is the external view of a music content record system.

[0023] The music content record system 1000 is a system which records the music content which received through the communication line 1001 on a memory card 1300. In addition, a personal computer 1100 can also reproduce the music content which received through a loudspeaker 1193. As the memory card 1300 was mentioned above, it is the medium which can record a music content including a flash memory, and a user can enjoy the music played through headphone etc. by inserting the memory card 1300 on which the music content was recorded in regenerative apparatus, such as a portable player.

[0024] As shown in this drawing, the music content record system 1000 consists of a personal computer 1100 equipped with a display 1191 and a keyboard 1192, and a memory card writer 1200 inserted in this. A personal computer 1100

contains CPU, memory, a hard disk, etc., and is connected with the communication line 1001, and it has the memory card writer insertion opening 1195 which is the so-called PC Card slot.

[0025] The memory card writer 1200 is the so-called PC card, and has the memory card insertion opening 1299 for inserting a memory card. Drawing 5 is the functional block diagram of the memory card writer 1200. In addition, functional block of a memory card 1300 is also shown in this drawing. Although the directions which a personal computer 1100 should download a music content from a communication line, and should record a specific music content on the predetermined pass of a memory card 1300 are given to the memory card writer 1200, in response, the memory card writer 1200 incorporates the specific music content enciphered from the personal computer 1100, decodes a music content, and has the function which gives encryption further for medium record etc. and is recorded on a memory card 1300. A specific music content is a music content of one music, and says the directory and file name in which predetermined pass stores a file.

[0026] In order to realize the above-mentioned function, the memory card writer 1200 It is what is equipped with an authentication circuit, WM extract circuit, a memory card interface circuitry, memory, CPU, etc. as hardware. Functionally The contents decode section 1201 which decodes the music content enciphered in order to secure the safety of the negotiation on a network, It has WM extract section 1202 which extracts WM for CGMS currently embedded at the music content as 2 bit data, and the Records Department 1210 which performs record to the memory card 1300 of a music content.

[0027] The Records Department 1210 has memorized the master key 1211 which is a peculiar key for encryption for every manufacturer, and has the file system 1220 containing the authentication section 1212, the media proper key storing section 1213, the file key generation section 1214, a file key and WM encryption section 1215, the contents encryption section 1216, and the logic access-control section 1221 and the physical access-control section 1222.

[0028] The authentication section 1212 performs a memory card 1300 and mutual recognition, obtains the media proper key which is a value peculiar to a memory card 1300 in the process of the mutual recognition using the master key 1211, and stores it in the media proper key storing section 1213 which is one field of memory. In addition, mutual recognition means attesting mutually the justification of the both sides of access equipment to a memory card and it here.

[0029] The file key generation section 1214 is what generates the 56-bit file key which is key data for encryption of the music content of one music based on a random number etc. The contents encryption section 1216 is what enciphers using a file key and outputs the music content decoded by the contents decode section 1201 to the logic access-control section 1221. The file key by which a file key and WM encryption section 1215 were generated by the file key generation section 1214, It enciphers with a DES algorithm using the media proper key in which it was stored by the media proper key storing section 1213, respectively, and WM extracted by WM extract section 1202 is outputted to the logic access-control section 1221 as 64-bit data, respectively.

[0030] The logic access-control section 1221 performs access directions in the physical access-control section 1222 so that the enciphered music content which was outputted to the memory card 1300 by the contents encryption section 1216 by the logical format shown in drawing 1 and drawing 2 may be recorded as data of a file unit and the encryption file key and Encryption WM which were outputted by a file key and WM encryption section 1215 may be recorded as a part of file entry.

[0031] Moreover, in response to the access directions by the logic access-control section 1221, to the access-control section 1320 which manages the access control of a flash memory 1330 in a memory card 1300, the physical access-control section 1222 is a block unit, specifies a block address and directs data read-out or writing. In addition, a block is a physical access unit in a flash memory 1330, and size is 2048 bytes.

[0032] On the other hand, a memory card 1300 is equipped with the

authentication section 1310 for performing mutual recognition with the access equipment to the memory card of memory card writer 1200 grade, the flash memory 1330 which can memorize data, and the access-control section 1320 which performs control of a flash memory 1330. In addition, drawing 6 is drawing having shown the internal configuration of a memory card 1300. Paying attention to the memory card 1300, it has expressed with the structure side to this drawing, and they are the authentication IN in this drawing, Authentication OUT, CLOCK, and ADDRESS. IN, DATA IN/OUT is an external pin and serves as a contact with the access equipment to the memory card concerned.

[0033] The authentication section 1310 is memorized into the part to which a user cannot access a master key peculiar to a manufacturer etc., and the media proper key 1312 of a medium proper, and performs a memory card writer etc. and mutual recognition with a challenge response procedure using these. In the process of mutual recognition, the authentication section 1310 transmits the media proper key (henceforth an encryption media proper key) enciphered using the master key to the authentication section 1212 of the memory card writer 1200, and the authentication section 1212 of the memory card writer 1200 decodes an encryption media proper key using the master key 1211, and it stores it in the media proper key storing section 1213.

[0034] The exterior carries out serial transmission of the data, and the access-control section 1320 writes a flash memory 1330 in the location which carries out parallel conversion of the serial data, and is shown by the block address concerned in a flash memory 1330, when parallel transmission is performed, a certain block address is specified from the physical access-control section 1222 of the memory card writer 1200 and serial data is sent per block.

[0035] Record processing of the music content to the memory card 1300 made by the memory card writer 1200 is explained below <record actuation of 2-2. data>. Drawing 7 is drawing showing the flow and reference data of the processing about record of the music content to a memory card 1300.

[0036] As shown in this drawing, record of the music content to a memory card

1300 is realized by authentication and the media proper key decode processing step S1510, an extract and file key of the file key generation processing steps S1520 and WM, and the encryption processing step S1530 of WM, and the record processing step S1540. The record processing step S1540 consists of a file entry write-in processing step S1541, and encryption of contents and the write-in processing step S1542 here.

[0037] The carrier beam memory card writer 1200 performs mutual recognition for record directions of a specific music content between the authentication sections 1310 of a memory card 1300 by the authentication section 1212 from a personal computer 1100, the encryption media proper key 1391 is obtained from a memory card 1300, and the media proper key 1601 which is the result of decoding this using the master key 1211 is stored in the media proper key storing section 1213 (step S1510).

[0038] The file key generation section 1214 generates the file key 1602 based on a random number after authentication and the media proper key decode processing step S1510 (step S1520). After the file key 1602 is generated, a file key and WM encryption section 1215 encipher WM extracted from the music content by WM extract section 1202, and the file key 1602 using the media proper key 1601, and generates the encryption file key 1603 and encryption WM1604 (step S1530).

[0039] The memory card writer 1200 after the encryption file key 1603 and generation of encryption WM1604 The pass information directed in the personal computer 1100 is followed using a file system 1220. A file entry including the encryption file key 1603 and encryption WM1604 is written in the flash memory 1330 of a memory card 1300 (step S1541). By moreover, the contents encryption section 1216 It enciphers using the file key 1602 and the contents outputted from the contents decode section 1201 are written in a flash memory 1330 (step S1542).

[0040] In the file entry write-in processing step S1541, the memory card writer 1200 stores the encryption file key 1603 and encryption WM1604, and stores 16

as a value of the encryption attribute field length field so that it may become the format shown in drawing 2 to the logic access-control section 1221 of a file system 1220. In addition, in the record processing step S1540, the information on others in a file entry follows a predetermined regulation, and is generated and updated. For example, the block address which has arranged the enciphered music content is stored in the AllocationDescriptors[] field. Moreover, on the occasion of file entry writing, additional storing of the file identification descriptor which set up the information which shows arrangement of a file name or a file entry is carried out to directory data.

[0041] Thus, the data which are a music content will be stored in the flash memory 1330 of a memory card 1300 by DS as shown in drawing 1 .

The memory card player which is beginning to read the music content recorded on the memory card by the music content record system mentioned above below <3. memory card player>, and plays music is explained.

[0042] <3-1. configuration> drawing 8 is the external view of a memory card player. The memory card player 2000 shown in this drawing can insert the memory card of two sheets, and it is equipment of the pocket mold which can edit playback of the music content recorded on the memory card, the copy of a music content, migration, etc., and has the liquid crystal display section 2001, a manual operation button 2002, and the memory card insertion openings 2011 and 2012, and headphone 2020 are connected.

[0043] A user can perform playback or edit directions by operating a manual operation button 2002, referring to the user interface display displayed on the liquid crystal display section 2001, and he can listen to the music outputted from headphone 2020, looking at the music name displayed on the liquid crystal display section 2001. Drawing 9 is the functional block diagram of the memory card player 2000.

[0044] In addition, functional block of a memory card 1300 is also shown in this drawing. In hardware the memory card player 2000 It is a thing equipped with an authentication circuit, a memory card interface circuitry, a D/A converter, memory,

CPU, etc. functionally The master key 2101 is memorized. The authentication section 2102 and the media proper key storing section 2103, A file key and WM decode section 2110, and the contents decode section 2111, It has the file system 2140 containing WM storing section 2112, the encryption section 2120 for deletion, the processing section 2130 for a copy, and the logic access-control section 2141 and the physical access-control section 2142, and the playback section 2150.

[0045] Since the master key 2101, the authentication section 2102, and the media proper key storing section 2103 are functionally equivalent to the master key 1211 in the memory card writer 1200, the authentication section 1212, and the media proper key storing section 1213, explanation is omitted here. As for a file key and WM decode section 2110, reading appearance of the file entry in the flash memory 1330 of a memory card 1300 is carried out by the logic access-control section 2141. If the encryption file key in a file entry and Encryption WM can be given The media proper key stored in the media proper key storing section 2103 by the authentication section 2102 is used. These are decoded, a file key is outputted to the contents decode section 2111, or the processing section for a copy and the encryption section 2120 for deletion, and WM is outputted to WM storing section 2112 which is one field of memory. In addition, when playback of a music content is required, the contents decode section 2111 is made to output a file key to a file key and WM decode section 2110, in response to user actuation, when the music content in a memory card needs a copy or moving, a file key is outputted to the processing section 2130 for a copy, and a memory card player outputs a file key to the encryption section 2120 for deletion, when migration or deletion is required.

[0046] If reading appearance of the enciphered music content which is a file in a flash memory 1330 is carried out by the logic access-control section 2141 and the contents decode section 2111 is given, it will decode the enciphered music content using the file key outputted by a file key and WM decode section 2110, and will output it to the playback section 2150.

[0047] A D/A converter etc. is realized, and the playback section 2150 changes and outputs a music content to the sound signal for a headphone input. From the memory card 1300 on which data are recorded in the logical format shown in drawing 1 and drawing 2, the logic access-control section 2141 performs access directions in the physical access-control section 2142 so that a file entry, the data which are a file may be read.

[0048] In response to the access directions by the logic access-control section 2141, to the access-control section 1320 which manages the access control of a flash memory 1330 in a memory card 1300, the physical access-control section 2142 is a block unit, specifies a block address and directs data read-out or writing. In case the encryption section 2120 for deletion deletes a moved material file with migration when deleting the file of the music content currently recorded in the memory card or, it enciphers a file key using a certain key of the others which are not media proper keys, and writes the encryption file key obtained by this in the encryption file key field of a file entry through the logic access-control section 2141.

[0049] After the processing section 2130 for a copy judges copy propriety of a music content and changes the value of WM with reference to WM stored in WM storing section 2112 if needed, a media proper key is used for it, it enciphers, generates Encryption WM, and it records Encryption WM as a value of the encryption WM field of the file entry of a copy place through the logic access-control section 2141.

[0050] Regeneration of the music content recorded on the memory card 1300 made by the memory card player 2000 is explained below <playback of 3-2. data>. Drawing 10 is drawing showing the flow and reference data of the processing about playback of a music content which were recorded on the memory card 1300.

[0051] As shown in this drawing, playback about the enciphered music content which is data recorded on the memory card 1300 as a file is realized by authentication and the media proper key decode processing step S2510, the file

entry read-out processing step S2520, the file key decode processing step S2530, and read-out of data, and decode and the regeneration step S2540 of contents.

[0052] The media proper key 2601 which is the result of the carrier beam memory card player's 2000 performing mutual recognition for playback directions of a specific file between the authentication sections 1310 of a memory card 1300 by the authentication section 2102, obtaining the encryption media proper key 1391 from a memory card 1300, and decoding this using the master key 2101 by the user is stored in the media proper key storing section 2103 (step S2510).

[0053] The memory card player 2000 reads the file entry used as the file in which playback directions were done by the user in a flash memory 1330, and a pair through a file system 2140 after authentication and the media proper key decode processing step S2510 (step S2520). Here, the encryption file key 2602 is contained in the read file entry. In addition, in the case of read-out of a file entry, the file identification descriptor which shows the arrangement is referred to. For example, in order to read the file entry 130 shown in drawing 1, it is necessary to carry out sequential access to the file set descriptor 103, the file entry 110 of a root directory, and the file identification descriptor 122.

[0054] After read-out of a file entry, by the file key and WM decode section 2110, the memory card player 2000 decodes the encryption file key 2602 using the media proper key 2601, and generates the file key 2603 (step S2530). Thereby, the file key 2603 is outputted to the contents decode section 2111. In step S2530, it checks that the content of the encryption attribute field length field in a file entry is 16, and when it is 16, the encryption file key of encryption file key field will be referred to. In addition, when the content of the encryption attribute field length field is not 16, the content of the file which is invalid as for the content of the encryption field, and serves as a file entry and a pair in this case is not enciphered. For example, the file in which the data in which the list of a music name or players is shown were stored is not enciphered.

[0055] After generation of the file key 2603, the memory card player 2000 reads the data which are the music content enciphered through the file system 2140 with reference to the AllocationDescriptors[] field of a file entry from a flash memory 1330, inputs them into the contents decode section 2111, is made to decode by the contents decode section 2111 using the file key 2603, obtains the raw music content 2604, and sends it to the playback section 2150 (step S2540).

[0056] Thus, the music content currently recorded on the flash memory 1330 of a memory card 1300 by DS as shown in drawing 1 will be reproduced.

The copy processing to the memory card 1400 of the data recorded on the memory card 1300 made by the memory card player 2000 as a file, i.e., the enciphered music content, is explained below a <3-3. copy of data>.

[0057] Drawing 11 is drawing showing the flow and reference data of the processing about the copy of data from a memory card 1300 to a memory card 1400. As shown in this drawing, the copy of the file from a memory card 1300 to a memory card 1400 is realized by authentication and the media proper key decode processing step S3010, the file entry read-out processing step S3020, a file key and WM decode processing step S3030, and encryption and file entry and the copy-of-data processing step S3040 of WM check, a file key, and WM.

[0058] Copy directions of the purport which should copy the specific file in a memory card 1300 to the specific pass in a memory card 1400 by the user the carrier beam memory card player 2000 The authentication section 2102 performs mutual recognition between the authentication sections 1310 of a memory card 1300. The encryption media proper key 1391 is obtained from a memory card 1300. The media proper key 3101 which is the result of decoding this using the master key 2101 is stored in the media proper key storing section 2103.

Moreover, also between the authentication sections 1410 of a memory card 1400, mutual recognition is performed and the media proper key 3105 of a memory card 1400 is similarly stored in the media proper key storing section 2103 (step S3010).

[0059] The memory card player 2000 reads the file entry used as the copied

material file specified by the user in a flash memory 1330, and a pair through a file system 2140 after authentication and the media proper key decode processing step S3010 (step S3020). In addition, in the read file entry 3102, as shown in drawing 2 , an encryption file key and Encryption WM are included.

[0060] The memory card player 2000 decodes the encryption file key and Encryption WM which are included in a file entry 3102 by the file key and WM decode section 2110 after read-out of a file entry using the media proper key 3101 of a memory card 1300, WM3103 obtained as a result of decode is stored in WM storing section 2112, and the file key 3104 obtained as a result of decode is outputted to the processing section 2130 for a copy (step S3030).

[0061] After storing WM3103 in WM storing section 2112, the memory card player 2000 performs copy-of-data processing by the processing section 2130 for a copy with encryption and the file entry of WM check and the file key which are shown below, and WM (step S3040). Drawing 12 is a flow chart which shows encryption of WM check, a file key, and WM, and a file entry and copy-of-data processing.

[0062] The processing section 2130 for a copy distributes processing with the value of WM with reference to WM3103 stored in WM storing section 2112 (step S3041). When WM3103 shows Free, it enciphers the file key 3104 and WM3103 using the media proper key 3105 of the memory card 1400 which is a copy place (step S3043), and creates a file entry with a file system 2140 to the flash memory 1430 of a memory card 1400 used as a copy place (step S3044). Creation of this file entry is performed by writing WM and the file key which were enciphered by step S3043 in the encryption WM field in a file entry 3102, and encryption file key field, and writing required information in other fields. The processing section 2130 for a copy copies the specific file of the memory card 1300 which is a copied material through a file system 2140 after creation of a file entry to the specific pass of the memory card 1400 which is a copy place, and the file entry created by step S3044 if needed is updated (step S3045).

[0063] Moreover, it sets to step S3041 and WM3103 is One. When Copy is

shown, it is No about the value of WM3103. More Step S3043 which changed into the value which shows Copy and was mentioned above after that - step S3045 are processed. Moreover, it sets to step S3041 and WM3103 is Never or NoMore. When Copy is shown, processing of step S3043 - step S3045 is skipped, and processing is ended.

[0064] Thus, the data which are one file stored in the flash memory 1330 of a memory card 1300 are copied to the flash memory 1430 of a memory card 1400. The migration processing to the memory card 1400 of the data recorded on the memory card 1300 made by the memory card player 2000 as a file, i.e., the enciphered music content, is explained below <migration of 3-4. data>. Migration is realized by deleting the file of a copied material after the above-mentioned copy.

[0065] Drawing 13 is drawing showing the flow and reference data of the processing about migration of the data from a memory card 1300 to a memory card 1400. In addition, in this drawing, the same sign as it in drawing 11 is attached about the thing equivalent to the case of processing of the copy of data from the above-mentioned memory card 1300 to a memory card 1400.

[0066] As shown in this drawing, migration of the file from a memory card 1300 to a memory card 1400 is realized by authentication and the media proper key decode processing step S3010, the file entry read-out processing step S3020, a file key and WM decode processing step S3030, encryption and the file entry of WM check, a file key, and WM, and the copy-of-data processing step S3040, and file key encryption and the update process step S3550.

[0067] Migration directions of the purport which should move the specific file in a memory card 1300 to the specific pass in a memory card 1400 by the user the carrier beam memory card player 2000 The authentication section 2102 performs mutual recognition between the authentication sections 1310 of a memory card 1300. The encryption media proper key 1391 is obtained from a memory card 1300. The media proper key 3101 which is the result of decoding this using the master key 2101 is stored in the media proper key storing section 2103.

Moreover, also between the authentication sections 1410 of a memory card 1400, mutual recognition is performed and the media proper key 3105 of a memory card 1400 is similarly stored in the media proper key storing section 2103 (step S3010).

[0068] The memory card player 2000 reads the file entry used as the copied material file specified by the user in a flash memory 1330, and a pair through a file system 2140 after authentication and the media proper key decode processing step S3010 (step S3020). In addition, in the read file entry 3102, as shown in drawing 2 , an encryption file key and Encryption WM are included.

[0069] After read-out of a file entry, the memory card player 2000 decodes the encryption WM included in a file entry 3102 by the file key and WM decode section 2110 using the media proper key 3101 of a memory card 1300, stores in WM storing section 2112 WM3103 obtained as a result of decode, decodes an encryption file key using the media proper key 3101 of a memory card 1300, and obtains the file key 3104 (step S3030).

[0070] After generating WM3103 and the file key 3104, the memory card player 2000 The processing section 2130 for a copy performs copy-of-data processing with encryption and the file entry of WM check, a file key, and WM (step S3040). By the encryption section 2120 for deletion The file key 3104 is enciphered using keys other than a media proper key. The encryption file key obtained as a result is written in the encryption file key field of the file entry about the file of a moved material with a file system 2140. Moreover, it updates so that it may be shown that it is deletion ending about the FileCharacteristics field of the file identification child (refer to drawing 1 and drawing 3) indicating the file entry concerned (step S3550).

[0071] Thus, the data which are one file stored in the flash memory 1330 of a memory card 1300 are copied to the flash memory 1430 of a memory card 1400, and are deleted about the file of a copied material. In addition, the encryption file key in the file entry about the deleted file is enciphered by keys other than a media proper key, because the music content which is the content of the file

cannot be reproduced even if it revives a deletion file by a certain approach. The logical DS of the digital work record medium (flash memory) concerning the gestalt 2 of operation of this invention is explained below the <gestalt 2 of operation>. UDF is used for the logical DS of the flash memory concerning the gestalt 2 of operation, and it defines the encryption flag field, encryption file key field, and the encryption WM field using the extended attribute field in a file entry. Therefore, it is the logical DS same except a file entry as the gestalt 1 of operation (refer to drawing 1 and drawing 3).

[0072] Drawing 14 is drawing showing the DS of the file entry concerning the gestalt 2 of operation. About the field of the same content as the file entry concerning the gestalt 1 of operation, the same sign is attached among this drawing, and the explanation is omitted. The ExtendedAttributes[] field 213 which is the field which can store two or more information which shows an extended attribute The DescriptorTag field 5101 and the ImplementationAttributesLocation field 5102, The ApplicationAttributesLocation field 5103, It consists of the implementationUseExtendedAttribute field 5104, 5105 grades, and the ApplicationUseExtendedAttribute field 5106 and 5107 grades.

[0073] Here, the DescriptorTag field 5101 is 16 bytes of field which stores the fixed value which shows the identifier of an extended attribute. The ImplementationUseExtendedAttribute field 5104 and 5105 grades are the variable-length fields which store an extended attribute with an usable system, respectively, and the head location is stored in the ImplementationAttributesLocation field 5102.

[0074] Moreover, the ApplicationUseExtendedAttribute field 5106 and 5107 grades are the variable-length fields where a user stores an usable extended attribute, respectively, and the head location is stored in the ApplicationAttributesLocation field 5103. In this drawing, ImplementationUseExtendedAttribute5105 The field of the extended attribute about a key, digital watermarking, etc. which were used for the encryption about a file (it is hereafter called code information field.) The example is shown. it is --

further the code information field concerned with the AttributeType field 5201 The AttributeSubType field 5202 and the Reserved field 5203, The AttributeLength field 5204 and the ImplementationUseLength field 5205, The ImplementationIdentifier field 5206, It consists of the HeaderChecksum field 5207, the encryption flag field 5208, the Reserved field 5209, encryption file key field 5210, and the encryption WM field 5211.

[0075] The AttributeType field 5201 and the AttributeSubType field 5202 are the fields where the classification of an extended attribute and sub classification are stored, and the fixed value 1000 and 10 which shows that they are code information field, for example, each, is stored in the example of this drawing. The Reserved fields 5203 and 5209 are the preliminary fields for future expansion etc.

[0076] The AttributeLength field 5204 is the field which stores the size of an extended attribute, and the content is set to 68 about code information field. The ImplementationUseLength field 5205 is the field which stores the size of all the fields following the ImplementationIdentifier field, and the content is set to 20 about code information field.

[0077] The ImplementationIdentifier field 5206 is the field which stores the identifier of an extended attribute, and serves as "**Flash Crypto Info" about code information field. It is the field which stores the information which shows whether the encryption flag field 5208 has the encryption file key field 5210 and the effective encryption WM field 5211, if the most significant bit is 1, validity is shown, and it is treated like the value of the encryption attribute field length field in the gestalt 1 of operation being 16.

[0078] About the encryption file key field 5210 and the encryption WM field 5211, it is equivalent in [as the encryption file key field 211 and the encryption WM field 212 in the gestalt 1 of operation] content. Moreover, the HeaderChecksum field 5207 is the field which stores the checksum of the value stored even in the encryption WM field 5211 from the encryption flag field 5208.

[0079] in addition, reference of the encryption file key in a file entry, and Encryption WM or updating, record of a file, and reading appearance -- carrying

out -- etc. -- record of the data explained with the gestalt 1 of operation, playback, a copy, and processing of migration and the same processing as a basic target can perform access to a flash memory. However, about the flash memory concerning the gestalt 2 of operation, a checksum is computed and stored in the HeaderChecksum field 5207 in the case of record of data, and suppose that the checksum concerned is checked in the case of read-out of data.

The logical DS of the digital work record medium (flash memory) concerning the gestalt 3 of operation of this invention is explained below the <gestalt 3 of operation>. The logical format of the FAT mold specified to X-JIS-0605 specification is used for the logical DS of the flash memory concerning the gestalt 3 of operation, and it stores the information about encryption of a file etc. using the free space of the directory item in a format of a common FAT mold.

[0080] Drawing 15 is drawing showing the DS of the directory item concerning the gestalt 3 of operation. The directory item 6100 has the magnitude of 32 bytes on the whole, and includes the file key +WM field 6102 enciphered as the encryption flag field 6101 which is the description of this invention further including each field of 11 bytes of file name, the attribute of a file, chart lasting time, a record date, a head cluster number, and file length.

[0081] if the attribute of a file shows that a directory item is a thing about a volume label including a volume label bit and a subdirectory bit if a volume label bit is 1, and a subdirectory bit is 1, a directory item is a thing about a subdirectory -- being shown -- any -- although -- if it is 0, it is shown that a directory item is a thing corresponding to a file.

[0082] If it is 1 bit of low order in 1 byte (8 bits) located in the 13th byte, it is the field which shows whether the content of the enciphered file key +WM field 6102 is effective, the 1 bit concerned is 1 and the encryption flag fields 6101 are validity and 0 when the head of the directory item 6100 is made into the 0th byte, they mean an invalid.

[0083] The enciphered file key +WM field 6102 is 8 bytes (64 bits) of field from the 14th byte of the directory item 6100 to the 21st byte, and are 64 bit data

which compound the 56 bits file key and 2-bit WM which were explained with the gestalt 1 of operation, encipher with a DES algorithm using a media proper key, and are obtained, i.e., the field which stores enciphered file key +WM.

[0084] About access to a flash memory, since the information relevant to the key of encryption, WM, etc. was only changed into the directory item from the file entry in the gestalt 1 of operation, the access control fundamentally shown in the gestalt 1 of operation is performed. That is, in enciphering a music content to a flash memory and recording on it as a file, after storing enciphered file key +WM which compounds WM embedded at the music content, and the file key used for encryption in the directory item corresponding to the file concerned, and is enciphered by the media proper key in it, it sets the content of the encryption flag field 6101 to 1.

[0085] Moreover, it sets to read-out of the data from a flash memory. When the content of the encryption flag field 6101 of a directory item is 1 and both the volume label bits and subdirectory bits of an attribute of a file are 0 Can judge that it is the file as which the file corresponding to a directory item was enciphered, and file key +WM enciphered from the enciphered file key +WM field is taken out. A file key and WM can be obtained by decoding using a media proper key. Using this file key, the music content which is the content of the file is decoded, it can reproduce, and the copy of a file etc. can be performed with reference to WM.

[0086] As mentioned above, although the DS of the digital work record medium concerning this invention and the access equipment to the record medium concerned were explained based on the gestalt of operation, as for this invention, it is needless to say that it is not restricted to the gestalt of these operations. That is, although [the gestalt 1 of (1) operation / the memory card writer 1200 which records audio data on a memory card] it is a PC card, it may not be limited to this, and you may be non-portable equipment, and may be equipment with portability. For example, the memory card player shown in the gestalt 1 of operation may be made to have a function as a memory card writer.

[0087] Moreover, in part, a function may be in a personal computer side and is good also as things for which software is used for a personal computer side and all the functions of a memory card writer are realized, such as the contents decode section shown in the memory card writer.

(2) With the gestalt 1 of operation, although a file key is generated based on a random number, according to the approach of generating a different file key to some extent for every file, it is not necessary to generate the file key generation section 1214 based on a random number. Moreover, the file key generation section 1214 is good also as generating a file key based on the random number which receives the kind of a random number from a memory card, and is generated by this.

(3) With the gestalt 1 of operation, although [the memory card writer 1200] a file key is enciphered using a media proper key, it is good also as enciphering a file key using the media proper key after conversion, after not being limited to this, receiving the password from a user and changing a media proper key using the password concerned. In this case, what is necessary is just to decode an encryption file key using the media proper key after conversion, after receiving the password from the user in the memory card player and changing a media proper key using the password concerned.

[0088] Moreover, are good also as using the subgroup key which is a key for encryption of the unit proper which the master key subordinate subdivided in addition to the master key in the gestalt 1 of operation. After a media proper key is changed by the authentication section of a memory card using a subgroup key, a master key is used for it and it is enciphered. In this case, as an encryption media proper key Are good also as memory card access equipments, such as a memory card writer or a memory card player, being given in the case of authentication. After memory card access equipment decodes an encryption media proper key using a master key corresponding to this, it is good also as obtaining a media proper key by using and transforming a subgroup key inversely.

[0089] Moreover, a media proper key is good also as using a subgroup key, being changed and being transmitted in process of authentication from the authentication section of a memory card, after being enciphered using a master key, and a media proper key is good also as being enciphered using the master key after being changed using the subgroup key, and being transmitted in process of authentication from the authentication section of a memory card. Also in this case, what is necessary is just to suppose memory card access equipment that a media proper key is obtained by performing inverse transformation and decode to these.

[0090] Furthermore, the key used for encryption of a file key is good also as being the combination of a subgroup key and a media proper key also as being a subgroup key.

(4) Although [the gestalten 1 and 2 of operation] WM is enciphered using a media proper key and it is stored in the encryption WM field of a file entry, it is good also as being enciphered using keys other than a media proper key. For example, it is good also as WM being enciphered using a file key. Moreover, the encryption file key and Encryption WM which are stored in encryption file key field and the encryption WM field are good also as being enciphered using a respectively different key. Moreover, WM is good also as being stored in the encryption WM field, without being enciphered.

[0091] Moreover, the encryption file key field and the encryption WM field in gestalten 1 and 2 of operation may be unified like the enciphered file key +WM field in the gestalt 3 of operation. That is, after mixing a file key and WM based on a predetermined regulation, it is good also as using a media proper key, enciphering and storing in the unified field.

(5) With the gestalten 1-3 of operation, although WM set to 2-bit CGMS, as long as it is digital watermarking which is not limited to this and embedded as a content of the file, it may be data which mean a copyright person name, an owner name, etc., and may be what bit data. However, when adopting a format of a FAT mold as shown in the gestalt 3 of operation as it is, the data size of WM

is restricted so that enciphered file key +WM may be settled in the free space of a directory item.

(6) Although a file key and the encryption algorithm of WM considered as the DES algorithm in the gestalten 1-3 of operation, it is good also as not being limited to this and using block encryption algorithms other than DES.

[0092] Moreover, the number of bits of a file key is not limited to 56 bits, either.

Therefore, especially the size of the encryption file key field shown in the gestalten 1 and 2 of operation and the encryption WM field is not limited to 8 bytes. Moreover, the bit position of the encryption flag shown with the gestalten 2 and 3 of operation may be any location.

(7) Although [the gestalten 1-3 of operation] a file key and WM were enciphered and it is contained in the file entry or directory item corresponding to a file, it is good also as either a file key or WM not existing. That is, the information relevant to WM is good also as not making it contain in a file entry or a directory item, and the information relevant to [without enciphering a file content] a file key is good also as not making it contain in a file entry or a directory item. What is necessary is just to consider as what the content of the encryption attribute field length field or the encryption flag field shows the existence of one existence for in these cases.

(8) Although the gestalten 1-3 of operation showed the logical DS of the data recorded on the flash memory of a memory card, this logical DS is applicable also in other record media other than a memory card. Moreover, the data which should be recorded as a file are not limited to a music content, but you may be other digital works and the file of a digital work and files, such as other management information, may be intermingled in a record medium.

(9) Although the pass information which shows the directory location which stores a file, and a file name shall be directed to a memory card writer from a personal computer with the gestalt 1 of operation, it is good also as a memory card writer determining a file name and a file storing location.

(10) Although [the gestalt 1 of operation] the music content of one music is

stored in one file, when units smaller than one music are handling units, such as a copy and a negotiation, in a unit smaller than one music, it is good for reverse also as one file, and the content of one file is not often as one file restrained [unit / than one music / larger] at the concept of music.

(11) With the gestalt 1 of operation, although migration processing of data was explained, a file key is updated by what cannot be decoded, i.e., the thing enciphered with other keys, about deletion of data as well as a part of data migration processing. In addition, the deleted file is good also as being moved to the directory, for example like a garbage can. Moreover, it is good also as enciphering not only a file key but WM with keys other than a media proper key in the case of migration and deletion.

[0093] In addition, when enciphering a file key or WM for the deletion accompanying migration, it is good also as using the media proper key of a migration place as a key of the encryption. Since the record medium of a migration place is needed by this in order to revitalize a deletion file, while reviving the file of the migration origin which checked and deleted existence of the file of a migration place at the time of revival, it is realizable in the function, i.e., the deletion file revival function in which the illegal copy was prevented, to delete the file of a migration place.

(12) Although the size of 1 block of a flash memory considered as 2048 bytes with the gestalten 1 and 2 of operation, not to be limited to this and what is necessary is just fixed sizes, such as 512 etc. bytes.

(13) Although [the gestalt 1 of operation] data transmission and reception are performed by serial transmission between access equipments, such as a memory card writer, and a memory card, you may be a transfer of 16 bit parallel, for example. In this case, the access-control section 1320 performs conversion of bus width of face, such as changing the data of a memory card 1300 and 16 bit parallel of access equipment Seki into 8 bits which is the data bit width of face of a flash memory, and conversion of signal level.

[0094] Moreover, the connection between access equipment and a memory card

is Universal. Serial General-purpose serial buses, such as Bus (USB), may be used, a memory card 1300 may carry out a direct difference to the connector of USB, and may load it, and a USB device can be inserted in a card slot, and it is making, and is made to perform mixture utilization with USB peripheral devices, such as a USB camera and a USB keyboard.

[0095] Moreover, you may transmit with IP protocol, using networks, such as Ethernet, as a serial bus. In this case, what is necessary is for IP protocol control section etc. just to perform IP protocol conversion in the interface part of a memory card.

(14) The record medium which recorded data by the DS shown in the gestalten 1-3 of operation may be set as the object of a negotiation and a sale.

[0096] Moreover, the record medium which recorded the machine program which realizes data logging as shown in the gestalt 1 of operation, data playback, a data copy, and the content of processing of data deletion may be set as the object of a negotiation and a sale. Although there are an IC card, an optical disk, a flexible disk, a ROM, etc. in a record medium, utilization is presented with said machine program recorded on these by being installed in the household-electric-appliances device which has a general purpose computer and a program execution function. That is, the household-electric-appliances device which has a general-purpose computer or a program execution function executes the installed above-mentioned machine program serially, and realizes data logging as shown in the gestalt of operation etc. In addition, the program described with the high level language for realizing the contents of processing, such as the above-mentioned data logging, can be circulated through a record medium, various channels, etc., such as a hard disk, and can also be distributed.

[0097]

[Effect of the Invention] The digital work record medium concerning this invention so that clearly from the above explanation It is the digital work record medium which recorded as a file the digital work data enciphered using the 1st key and in which computer reading is possible. The management information field as a

logical field which recorded the management information which corresponds to said file and includes the information about the record location of the file concerned is included. It is characterized by said management information field including the field which recorded further the 1st key of encryption which enciphers said 1st key using the 2nd key.

[0098] Since this records the 1st key used for encryption of the content of the file on the management information field which is a logical field, it cannot be dependent on characteristic DS, such as contents which are not dependent on the physical structure of a record medium, and serve as a file content, etc., and the 1st key, i.e., a file key, can be enciphered and recorded. A management information field is a file entry in UDF here, and since the read-out equipment of a file is what accesses a file by referring to this file entry, read-out of the enciphered file key which was logically positioned by refer to the file entry and coincidence in the file entry of it usually becomes possible. Therefore, the read-out equipment of a file can decode a file content promptly by decoding the enciphered file key and obtaining a file key using a file key.

[0099] That is, since speeding up of decode of the file concerned can be attained according to the above-mentioned record format when a file content is enciphered using a different key for encryption per file, in order to raise the security of a digital work, it can be said that the digital work is recorded by the optimal DS in a security side and a utilization side.

[0100] Moreover, also suppose that said 2nd key is independently recorded on the field different from the 1st key of encryption. Thereby, since the key for encryption of a file key is contained in the record medium, by acquiring this key, the equipment which accesses the record medium concerned can decode a file key, and can also decode the content of the file.

[0101] Moreover, also suppose said management information field that the field which recorded the encryption existence flag which shows whether the content of the field which recorded said 1st key of encryption is still more effective is included. The encryption flag which is the information about whether the

enciphered file key is recorded effectively by this For example, since it is stored all over the management information field of formats, such as a file entry, In order to access a file, when the equipment which accesses a record medium refers to a management information field, it can refer to an encryption flag and can judge whether the file is enciphered or it is not carried out based on an encryption flag. in this case, when the purport on which the file key as which the encryption flag was enciphered is recorded effectively is shown, said equipment Since it is enciphered, the content of the file concerned decodes said enciphered file key. When the purport on which the file key as which the content of the file concerned could be decoded and used using this, and the encryption flag was enciphered is not recorded effectively is shown Since it is not enciphered, the content of the file concerned can use the content of the file concerned as it is.

[0102] Moreover, the digital work record medium concerning this invention is the digital work record medium which recorded as a file the digital work data with which digital watermarking was embedded and in which computer reading is possible, and it is characterized by for said management-information field to include the field which recorded the information showing said digital watermarking further including the management-information field as a logical field which recorded the management information which corresponds to said file and includes the information about the record location of the file concerned.

[0103] Thereby, the equipment which performs the copy of the file in the record medium concerned etc. since WM is recorded all over the management information field in a record medium does not need to extract WM from the enciphered digital work data which are a file content directly, and refer to the WM for it easily. Although it has the fault that the circuit magnitude of the circuit for WM extract is also large, its power consumption is also high, and an extract takes time amount, when it is not necessary to build in the circuit for WM extract, and small lightweight-ization can be attained and said WM includes the information about the copy propriety of a file, since said equipment can refer to the WM concerned easily, according to this invention, the quick copy of it etc. is

attained.

[0104] Moreover, said digital watermarking is the information about said digital work copy-of-data propriety, and the information showing said digital watermarking can also presuppose that it is said digital watermarking encryption digital watermarking enciphered using the 2nd key. In order for this to record what enciphered WM all over a management information field, WM is protected from an unjust peep and the difficulty of an alteration of WM also increases. Moreover, WM is the information about the copy propriety of a file, and since copy propriety can be simultaneously judged when a management information field is referred to from being recorded all over a management information field, in order to acquire the information about the file which should be copied, a file can be copied promptly.

[0105] Moreover, the digital work record medium concerning this invention It is the digital work record medium which recorded as a file what enciphered the digital work data with which digital watermarking was embedded using the 1st key and in which computer reading is possible. The management information field as a logical field which recorded the management information which corresponds to said file and includes the information about the record location of the file concerned is included. It is characterized by said management information field including the field which recorded further the 1st key of encryption which enciphers said 1st key using the 2nd key, and the field which recorded what enciphered said digital watermarking using said 1st key or said 2nd key.

[0106] Since this both records the 1st key used for encryption of the content of the file, and WM currently embedded by the content of the file on the management information field which is a logical field, it cannot be dependent on characteristic DS, such as contents which are not dependent on the physical structure of a record medium, and serve as a file content, etc., and the 1st key and WM can be enciphered and recorded. Therefore, since the equipment which accesses a record medium can obtain the 1st enciphered key and enciphered

WM while it acquires the positional information of a file if a management information field is accessed, it can perform decode of a file content etc. promptly.

[0107] Moreover, also suppose said management information field that the field which enciphered and recorded what doubled said 1st key and said digital watermarking using said 2nd key is included. Thereby, since what was enciphered after a file key and WM were mixed is recorded in the management information field of a record medium, if the alteration of WM is made, a file key will be destroyed and security will increase in it.

[0108] Moreover, also suppose said digital work record medium that it has the active component which performs mutual recognition further between the equipment which accesses the digital work record medium concerned. Since it may be accessed by the file by this only when it succeeds in authentication, security increases.

[0109] Moreover, further, said digital work record medium has the active component which performs mutual recognition between the equipment which accesses the digital work record medium concerned, and said 2nd key is a key of a value peculiar to said digital work record medium, and it can also presuppose it that what enciphered said 2nd key from said digital work record medium in the process of said mutual recognition is transmitted to said equipment.

[0110] Since it may be accessed by this only from the equipment which succeeded in authentication, security increases. Moreover, since a record medium gives the key for decode of the 1st enciphered key or enciphered WM in an authentication process, the equipment which accesses the record medium concerned can decode the 1st key or WM, when it succeeds in authentication. Moreover, said file is Universal. Disk It is recorded according to Format and said management information field is Universal. Disk It is a file entry in Format and also suppose that it is the field which recorded said 1st key of encryption an extended attribute field in said file entry.

[0111] Thereby, the file in a record medium can be operated now from the access equipment corresponding to UDF. Moreover, if expansion of the access

equipment corresponding to UDF is carried out, it can perform decoding the content of the enciphered file etc. Moreover, also suppose that it is the field which said file was recorded according to the FAT mold format in said digital work record medium, and said management information field is a directory item in a FAT mold format of JIS-X-0605 specification, and recorded said 1st key of encryption a free space in said directory item.

[0112] Thereby, the file in a record medium can be operated now from the access equipment corresponding to a FAT mold format. Moreover, if expansion of the access equipment corresponding to a FAT mold format is carried out, it can perform decoding the content of the enciphered file etc. The recording apparatus concerning this invention to moreover, a record medium equipped with the active component which has an authentication function An authentication means to be the recording device which records as a file the digital work data enciphered after the authentication success, and to perform said record medium and mutual recognition, A file record means to record on said record medium by considering said digital work enciphered using the 1st key as a file, it is characterized by being one logically, and including said 1st key enciphered using the 2nd key, and the information about the record location of said file in the management information field corresponding to the file concerned by 1 to 1, and recording them on said record medium.

[0113] Since this records the 1st key used for encryption of the content of the file on the management information field which is a logical continuation field, it cannot be dependent on characteristic DS, such as contents which are not dependent on the physical structure of a record medium, and serve as a file content, etc., and the 1st key, i.e., a file key, can be enciphered and recorded. Moreover, the regenerative apparatus concerning this invention is equipped with the active component which has an authentication function. And the digital work data enciphered using the 1st key are recorded as a file. and from the record medium with which what said 1st key was enciphered as using the 2nd key, and the information about the record location of the file concerned are recorded on

the logical management information field An authentication means to be the regenerative apparatus which reads and decodes the enciphered digital work data concerned, and is reproduced after an authentication success, and to perform said record medium and mutual recognition, A 1st key decode means to read said 1st enciphered key which is recorded on said management information field, and to decode using said 2nd key, The enciphered digital work data which are recorded as said file are read, and it is characterized by having a data decode playback means to decode and reproduce using the 1st key decoded by said 1st key decode means.

[0114] Since the enciphered file key which was logically positioned in the management information field can be read while referring to a management information field by this, in order to acquire the positional information of a file, by decoding the enciphered file key and obtaining a file key, using a file key, a regenerative apparatus can decode a file content promptly and can be reproduced.

[0115] Moreover, the deletion equipment concerning this invention is equipped with the active component which has an authentication function. And the digital work data enciphered using the 1st key are recorded as a file. and from the record medium with which the deletion information which shows whether what said 1st key was enciphered as using the 2nd key, the information about the record location of the file concerned, and the file concerned are deleted is recorded on the logical management information field An authentication means to be deletion equipment which deletes the enciphered digital work data concerned logically after an authentication success, and to perform said record medium and mutual recognition, Read said 1st enciphered key which is recorded on said management information field, and said 1st key decoded and obtained using said 2nd key is enciphered with said 2nd key and the 3rd different key. It records on said read location and is characterized by updating so that the purport from which a file is deleted in said deletion information in said management information field may be shown.

[0116] [when this deletes a file logically by rewriting of the content of the management information field] Since it is what is enciphered using the 2nd key which usually uses for encryption the 1st enciphered key, i.e., the enciphered file key, and 3rd another different key, Also when a file is revived by rewriting of the content of the management information field even if, a file key cannot be decoded with the decode means which used the 2nd usual key. When moving the file which makes the content the digital work with which it follows, for example, the copy is forbidden to another record medium from a certain record medium, in order to delete the file of migration-after copy origin at a high speed, even if it is a time of using the approach of logical deletion, the situation which the file deleted by a certain actuation revives, and exists in two duplicates of the digital work which can be used can prevent.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the logical DS of the digital work record medium (flash memory) concerning the gestalt 1 of operation of this invention.

[Drawing 2] It is drawing showing the DS of a file entry.

[Drawing 3] It is drawing showing the DS of a file identification descriptor.

[Drawing 4] It is the external view of a music content record system.

[Drawing 5] It is the functional block diagram of the memory card writer 1200.

[Drawing 6] It is drawing showing the internal configuration of a memory card 1300.

[Drawing 7] It is drawing showing the flow and reference data of the processing about record of the music content to a memory card 1300.

[Drawing 8] It is the external view of a memory card player.

[Drawing 9] It is the functional block diagram of the memory card player 2000.

[Drawing 10] It is drawing showing the flow and reference data of the processing about playback of a music content which were recorded on the memory card 1300.

[Drawing 11] It is drawing showing the flow and reference data of the processing about the copy of data from a memory card 1300 to a memory card 1400.

[Drawing 12] It is the flow chart which shows encryption of WM check, a file key, and WM, and a file entry and copy-of-data processing.

[Drawing 13] It is drawing showing the flow and reference data of the processing about migration of the data from a memory card 1300 to a memory card 1400.

[Drawing 14] It is drawing showing the DS of the file entry concerning the gestalt 2 of operation.

[Drawing 15] It is drawing showing the DS of the directory item concerning the gestalt 3 of operation.

[Description of Notations]

101 Volume Structure Information

102 Volume Structure Information is Copy Part.

103 File Set Descriptor

121, 122, 123 File identification descriptor

110 130 File entry

140, 150, 160 Data

210 Encryption Attribute Field Length Field

211 Encryption File Key Field

212 Encryption WM Field

1200 Memory Card Writer

1201 Contents Decode Section

1202 WM Extract Section

1210 Records Department

1211 Master Key

1212 Authentication Section

1213 Media Proper Key Storing Section

1214 File Key Generation Section
1215 WM Encryption Section
1216 Contents Encryption Section
1220 File System
1221 Logic Access-Control Section
1222 Physical Access-Control Section
1300 Memory Card
1310 Authentication Section
1312 Media Proper Key
1320 Access-Control Section
1330 Flash Memory
2000 Memory Card Player
2101 Master Key
2102 Authentication Section
2103 Media Proper Key Storing Section
2110 WM Decode Section
2111 Contents Decode Section
2112 WM Storing Section
2120 Encryption Section for Deletion
2130 Processing Section for Copy
2140 File System
2141 Logic Access-Control Section
2142 Physical Access-Control Section
2150 Playback Section
5208 Encryption Flag Field
5210 Encryption File Key Field
5211 Encryption WM Field
6100 Directory Item
6101 Encryption Flag Field
6102 Enciphered File Key +WM Field

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-163882

(P2000-163882A)

(43) 公開日 平成12年6月16日 (2000.6.16)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
G 1 1 B 20/12		G 1 1 B 20/12	5 B 0 1 7
G 0 6 F 12/00	5 3 7	G 0 6 F 12/00	5 3 7 H 5 B 0 3 5
12/14	3 2 0	12/14	3 2 0 E 5 B 0 5 8
			3 2 0 B 5 B 0 8 2
G 0 6 K 17/00		G 0 6 K 17/00	B 5 C 0 7 6
審査請求 未請求 請求項の数14 O L (全 23 頁) 最終頁に続く			

(21) 出願番号 特願平10-340487

(22) 出願日 平成10年11月30日 (1998.11.30)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 廣田 照人

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 小塚 雅之

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 100090446

弁理士 中島 司朗 (外1名)

最終頁に続く

(54) 【発明の名称】 デジタル著作物記録媒体並びに当該記録媒体にアクセスする記録装置、再生装置及び削除装置

(57) 【要約】

【課題】 セキュリティ面と利用面において最適なデータ構造でデジタル著作物が記録されたデジタル著作物記録媒体を提供する。

【解決手段】 ファイル毎に異なるファイルキーを用いて暗号化されたデジタル著作物データをファイルとして記録し、当該ファイルに対応するアクセス用管理情報であるファイルエントリ中の暗号化ファイルキーフィールド211に、前記ファイルキーを、記録媒体固有の鍵であるメディア固有キーを用いて暗号化して得られる暗号化ファイルキーを記録する。

ファイルエントリ

	フィールド名	長さ
201	DescriptorTag	16
202	ICBTag	20
203	Uid	4
204	Gid	4

205	AccessTime	12
206	ModificationTime	12

207	UniqueID	8
208	LengthOfExtendedAttributes	4
209	LengthOfAllocationDescriptors	4
210	暗号化属性領域長	4
211	暗号化ファイルキー	8
212	暗号化WM	8
213	ExtendedAttributes[]	可変長
214	AllocationDescriptors[]	可変長

【特許請求の範囲】

【請求項1】 第1鍵を用いて暗号化されたデジタル著作物データをファイルとして記録したコンピュータ読み取り可能なデジタル著作物記録媒体であって、前記ファイルに対応し当該ファイルの記録位置に関する情報を含む管理情報を記録した論理的な領域としての管理情報領域を含み、前記管理情報領域はさらに、前記第1鍵を、第2鍵を用いて暗号化したものである暗号化第1鍵を記録した領域を含むことを特徴とするデジタル著作物記録媒体。

【請求項2】 前記第2鍵は、暗号化第1鍵とは別の領域に単独で記録されていることを特徴とする請求項1記載のデジタル著作物記録媒体。

【請求項3】 前記管理情報領域はさらに、前記暗号化第1鍵を記録した領域の内容が有効か否かを示す暗号化有無フラグを記録した領域を含むことを特徴とする請求項1又は2記載のデジタル著作物記録媒体。

【請求項4】 電子透かしが埋め込まれたデジタル著作物データをファイルとして記録したコンピュータ読み取り可能なデジタル著作物記録媒体であって、前記ファイルに対応し当該ファイルの記録位置に関する情報を含む管理情報を記録した論理的な領域としての管理情報領域を含み、前記管理情報領域はさらに、前記電子透かしを表す情報を記録した領域を含むことを特徴とするデジタル著作物記録媒体。

【請求項5】 前記電子透かしは前記デジタル著作物データのコピー可否に関する情報であり、前記電子透かしを表す情報は、前記電子透かしを、第2鍵を用いて暗号化したものである暗号化電子透かしであることを特徴とする請求項4記載のデジタル著作物記録媒体。

【請求項6】 電子透かしが埋め込まれたデジタル著作物データを、第1鍵を用いて暗号化したものをファイルとして記録したコンピュータ読み取り可能なデジタル著作物記録媒体であって、前記ファイルに対応し当該ファイルの記録位置に関する情報を含む管理情報を記録した論理的な領域としての管理情報領域を含み、前記管理情報領域はさらに、前記第1鍵を、第2鍵を用いて暗号化したものである暗号化第1鍵を記録した領域と、前記電子透かしを前記第1鍵又は前記第2鍵を用いて暗号化したものを記録した領域とを含むことを特徴とするデジタル著作物記録媒体。

【請求項7】 前記管理情報領域は、前記第1鍵と前記電子透かしとを合わせたものを前記第2鍵を用いて暗号化して記録した領域を含むことを特徴とする請求項6記載のデジタル著作物記録媒体。

【請求項8】 前記デジタル著作物記録媒体はさらに、

当該デジタル著作物記録媒体にアクセスする装置との間で相互認証を実行するアクティブ素子を有することを特徴とする請求項4記載のデジタル著作物記録媒体。

【請求項9】 前記デジタル著作物記録媒体はさらに、当該デジタル著作物記録媒体にアクセスする装置との間で相互認証を実行するアクティブ素子を有し、前記第2鍵は、前記デジタル著作物記録媒体に固有な値の鍵であり、前記相互認証の過程において前記デジタル著作物記録媒体から前記第2鍵を暗号化したものが前記装置に送信されることを特徴とする請求項1～3、5～7のいずれか1項に記載のデジタル著作物記録媒体。

【請求項10】 前記ファイルはUniversal Disk Formatに従って記録されており、前記管理情報領域は、Universal Disk Formatにおけるファイルエントリであり、前記暗号化第1鍵を記録した領域は、前記ファイルエントリ中の拡張属性領域であることを特徴とする請求項1記載のデジタル著作物記録媒体。

【請求項11】 前記デジタル著作物記録媒体において前記ファイルはFAT型フォーマットに従って記録されており、前記管理情報領域は、JIS-X-0605規格のFAT型フォーマットにおけるディレクトリ項目であり、前記暗号化第1鍵を記録した領域は、前記ディレクトリ項目中の未使用領域であることを特徴とする請求項1記載のデジタル著作物記録媒体。

【請求項12】 認証機能を有するアクティブ素子を備える記録媒体に、認証成功後に暗号化されたデジタル著作物データをファイルとして記録する記録装置であって、前記記録媒体と相互認証を行う認証手段と、第1鍵を用いて暗号化された前記デジタル著作物をファイルとして前記記録媒体に記録するファイル記録手段と、第2鍵を用いて暗号化された前記第1鍵と、前記ファイルの記録位置に関する情報とを論理的に一体でありかつ当該ファイルに1対1で対応する管理情報領域に含めて、前記記録媒体に記録することを特徴とする記録装置。

【請求項13】 認証機能を有するアクティブ素子を備え、かつ、第1鍵を用いて暗号化されたデジタル著作物データがファイルとして記録され、かつ、前記第1鍵が第2鍵を用いて暗号化されたものと当該ファイルの記録位置に関する情報とが論理的な管理情報領域に記録されている記録媒体から、認証成功後に、当該暗号化されたデジタル著作物データを読み出して復号して再生する再生装置であって、前記記録媒体と相互認証を行う認証手段と、

前記管理情報領域に記録されている暗号化された前記第1鍵を読み出し、前記第2鍵を用いて復号する第1鍵復号手段と、

前記ファイルとして記録されている暗号化されたデジタル著作物データを読み出し、前記第1鍵復号手段により復号された第1鍵を用いて復号して再生するデータ復号再生手段とを備えることを特徴とする再生装置。

【請求項14】 認証機能を有するアクティブ素子を備え、かつ、第1鍵を用いて暗号化されたデジタル著作物データがファイルとして記録され、かつ、前記第1鍵が第2鍵を用いて暗号化されたものと当該ファイルの記録位置に関する情報と当該ファイルが削除されたものであるか否かを示す削除情報とが論理的な管理情報領域に記録されている記録媒体から、認証成功後に、当該暗号化されたデジタル著作物データを論理的に削除する削除装置であって、

前記記録媒体と相互認証を行う認証手段と、

前記管理情報領域に記録されている暗号化された前記第1鍵を読み出し、前記第2鍵を用いて復号して得られる前記第1鍵を前記第2鍵と異なる第3鍵で暗号化して、前記読み出した位置に記録し、

前記管理情報領域中の前記削除情報を、ファイルが削除されたものである旨を示すように更新することを特徴とする削除装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、デジタル著作物を記録するための記録媒体のデータ構造に関し、また、当該記録媒体へのアクセス装置に関する。

【0002】

【従来の技術】 近年、マルチメディア・ネットワーク技術の発展により、デジタル著作物である音楽等のコンテンツがインターネット等を通じて配信されるようになり、自宅に居ながらにして世界中の音楽等に接することが可能となってきた。また、このような音楽コンテンツ等は、半導体メモリ等の記憶媒体に記録することも可能である。半導体メモリ等の記録媒体に記録された音楽等のコンテンツは、例えば、携帯型の音楽再生装置により読み出され再生される。

【0003】 ところで、記録媒体にデータを記録する場合、内容的にまとまりあるデータをその単位で取扱いやすくするためファイルの概念を用い、記録媒体にはデータのまとまりであるファイルと、ファイルを管理するための管理情報とを対にして記録することができる。管理情報は、例えばファイルについてのアクセス可否等の属性やサイズやファイル位置等を示す情報であり、この管理情報を参照することによりファイルへのアクセスを行うことができる。

【0004】 記録媒体に記録されるデジタル著作物は、不正利用から有効に保護されるべきであり、インタ

ーネット等を通じて安全確実なコンテンツ配信を実現するためには、暗号化、電子透かし等のセキュリティ技術が用いられる。

【0005】

【発明が解決しようとする課題】 しかしながら、従来、コンテンツ配信に関してのセキュリティ技術は開発されたが、コンテンツを記録媒体に記録する際におけるフォーマット、即ち記録媒体のデータ構造についての上記セキュリティ技術の具体化は不十分であり、現在、ファイルとしてコンテンツを記録する場合において、コンテンツの著作権者や権利者の保護とコンテンツの利用の容易化とを図るための最適なデータ構造が求められている。

【0006】 そこで、本発明は、このような要請に鑑みてなされたものであり、セキュリティ面と利用面とにおいて最適なデータ構造でデジタル著作物が記録されたデジタル著作物記録媒体を提供することを目的とする。

【0007】

【課題を解決するための手段】 上記課題を解決するために本発明に係るデジタル著作物記録媒体は、第1鍵を用いて暗号化されたデジタル著作物データをファイルとして記録したコンピュータ読み取り可能なデジタル著作物記録媒体であって、前記ファイルに対応し当該ファイルの記録位置に関する情報を含む管理情報を記録した論理的な領域としての管理情報領域を含み、前記管理情報領域はさらに、前記第1鍵を、第2鍵を用いて暗号化したものである暗号化第1鍵を記録した領域を含むことを特徴とする。

【0008】 上記構成により、ファイルの内容の暗号化に用いた第1鍵を論理的な領域である管理情報領域に記録するため、記録媒体の物理的構造に依存せず、また、ファイル内容となるコンテンツ等の特有のデータ構造等にも依存せず、第1鍵、即ちファイルキーを暗号化して記録することができる。また、本発明に係るデジタル著作物記録媒体は、電子透かしが埋め込まれたデジタル著作物データをファイルとして記録したコンピュータ読み取り可能なデジタル著作物記録媒体であって、前記ファイルに対応し当該ファイルの記録位置に関する情報を含む管理情報を記録した論理的な領域としての管理情報領域を含み、前記管理情報領域はさらに、前記電子透かしを表す情報を記録した領域を含むことを特徴とする。

【0009】 上記構成により、電子透かしが、記録媒体における管理情報領域中に記録されているため、当該記録媒体中のファイルのコピー等を行う装置は、ファイル内容である暗号化されたデジタル著作物データから直接的に電子透かしを抽出する必要なく、容易に電子透かしを参照することができる。電子透かし抽出用の回路は回路規模も大きく、消費電力も高く、抽出に時間がかかるという欠点をもつが、本発明によれば前記装置は、電

子透かし抽出用の回路を内蔵する必要がなく、小型軽量化が図れ、また、前記電子透かしがファイルのコピー可否に関する情報を含む場合には、容易に当該電子透かしを参照することができるため迅速なコピー等が可能となる。

【0010】

【発明の実施の形態】以下、本発明に係るデジタル著作物記録媒体のデータ構造について、図面を用いて説明する。

<実施の形態1>

<1. フラッシュメモリ内のデータ構造>図1は、本発明の実施の形態1に係るデジタル著作物記録媒体（フラッシュメモリ）の論理的データ構造を示す図である。

【0011】同図に示すフラッシュメモリは、デジタル著作物を記録可能なICカード（以下、メモリカードという。）の一部であり、データの書き込み及び読み出しが可能な64メガバイトの記憶容量をもつフラッシュメモリである。なお、メモリカードは、厚さ数ミリ、縦横2cm四方程度の形状で、フラッシュメモリの他に、相互認証、フラッシュメモリのアクセス制御等の機能をもつアクティブ素子を有する。

【0012】フラッシュメモリには、UDF（Universal Disk Format）に類似した論理フォーマットで各種情報が格納される。即ち、ボリューム構造情報101、ボリューム構造情報の一部コピー102、ファイルセット記述子103、ルートのファイルエントリ110、ディレクトリデータ120の他、必要に応じてファイルエントリ130、データ140、150、160等が格納される。

【0013】ボリューム構造情報101は、記録媒体全体に関する情報であり、全体容量等の情報を含む。ファイルセット記述子103は、ルートのファイルエントリ110の配置を示す情報やファイル名に用いる文字コード等の情報を含む。ルートのファイルエントリ110は、ルートディレクトリのファイルエントリでありディレクトリデータ120の配置を示す。

【0014】ディレクトリデータ120は、ファイルエントリの配置やファイル名を示すファイル識別記述子121、122、123の集合である。同図には、ファイル識別記述子122がファイルエントリ130の配置を示す情報を含む様子を示している。ファイルエントリ130は、ファイルを構成するデータ140、150、160の配置を示す情報を含む。なお、ファイルエントリはデータ又はディレクトリデータと対となって存在する。

【0015】図2は、ファイルエントリのデータ構造を示す図である。ファイルエントリは、DescriptorTagフィールド201、ICBTagフィールド202、Uidフィールド203、Gidフィールド204、AccessTimeフィールド205、Mod

ificationTimeフィールド206、UniqueIDフィールド207、LengthOfExtendedAttributesフィールド208、LengthOfAllocationDescriptorsフィールド209、暗号化属性領域長フィールド210、暗号化ファイルキーフィールド211、暗号化WMフィールド212、ExtendedAttributes[]フィールド213、AllocationDescriptors[]フィールド214等を含むもので、そのサイズは基本的に2048バイトである。暗号化属性領域長フィールド210、暗号化ファイルキーフィールド211、暗号化WMフィールド212がUDFと相違し本発明の特徴となる部分である。

【0016】DescriptorTagフィールド201は、ファイルエントリであることを示す所定の識別子を格納するフィールドであり、ICBTagフィールド202は、ファイルの種類や属性を示す情報を格納するフィールドであり、Uidフィールド203は、ファイルの所有者の識別子を格納するフィールドであり、Gidフィールド204は、ファイルのグループの識別子を格納するフィールドである。

【0017】AccessTimeフィールド205は、ファイルを読み出した時刻を示す情報を格納するフィールドであり、ModificationTimeフィールド206は、ファイルを更新した時刻を示す情報を格納するフィールドであり、UniqueIDフィールド207は、ファイル固有の識別子を格納するフィールドである。

【0018】ExtendedAttributes[]フィールド213は、拡張属性を示す情報を複数格納できるフィールドであり、LengthOfExtendedAttributesフィールド208は、ExtendedAttributes[]フィールド213の領域サイズを格納するフィールドである。AllocationDescriptors[]フィールド214は、ファイルの配置を示す情報を格納するフィールドであり、例えば図1に示すファイルエントリ130のAllocationDescriptors[]フィールドは、データ140、150、160の配置を示す情報を格納している。LengthOfAllocationDescriptorsフィールド209は、AllocationDescriptors[]フィールド213の領域サイズを格納するフィールドである。

【0019】暗号化ファイルキーフィールド211は、ファイルの内容であるデータの暗号化に用いられたキーである56ビットのファイルキーにDES（Data Encryption Standard）アルゴリズムにより暗号化を施した結果得られる64ビットデータ（以下、暗号化ファイルキーという。）を格納する8バ

イトのフィールドであり、暗号化WMフィールド212は、ファイルの内容であるデータに含まれる電子透かし（以下、WM（WaterMark）という。）が抽出され暗号化されたものを格納する8バイトのフィールドである。ここでは、WMは、DVDにおいてコンテンツデータに埋め込まれているCGMS（Copy Generation Management System）と同様の2ビットデータとし、暗号化WMフィールド212には、当該2ビットデータにDESアルゴリズムにより暗号化を施して得られる64ビットデータ（以下、暗号化WMという。）を格納するものとする。

【0020】なお、CGMSの2ビットデータは、コピー自由（Free）、コピー禁止（Never）、1度のみコピー可能（One Copy）、1度コピー済みで更なるコピー禁止（No More Copy）のいずれかを意味する値をとる。また、暗号化属性領域長フィールド210は、暗号化ファイルキーフィールド211及び暗号化WMフィールド212のサイズを格納して、これらのフィールドに格納された値が有効か否かを示すものであり、値が16の場合には、暗号化ファイルキー及び暗号化WMが有効であり、値が0の場合には、暗号化ファイルキー及び暗号化WMは無効であることを意味する。

【0021】図3は、ファイル識別記述子のデータ構造を示す図である。ファイル識別記述子は、例えばディレクトリデータ120を構成し（図1参照）、ファイルエントリを指し示す情報を含むものであり、図3に示すようにFileCharacteristicsフィールド301、ICBフィールド302、FileIdentifierフィールド303等からなる。ここで、ICBフィールド302はファイルエントリの配置を示すブロックアドレスを格納するフィールドであり、FileCharacteristicsフィールド301は、ファイルが削除済みファイルであるか、ディレクトリであるかを示す情報を格納するフィールドであり、FileIdentifierフィールド303は、ファイル名又はディレクトリ名を示す情報が格納されるフィールドである。

【0022】＜2. 音楽コンテンツ記録システム＞以下、音楽コンテンツを、メモリカードに上述したデータ構造で記録する音楽コンテンツ記録システムについて説明する。

＜2-1. 構成＞図4は、音楽コンテンツ記録システムの外観図である。

【0023】音楽コンテンツ記録システム1000は、通信回線1001を介して受信した音楽コンテンツをメモリカード1300に記録するシステムである。なお、パーソナルコンピュータ1100は、受信した音楽コンテンツをスピーカ1193を介して再生することもできる。メモリカード1300は、上述したようにフラッシ

ュメモリを含み、音楽コンテンツの記録が可能な媒体であり、ユーザは、音楽コンテンツが記録されたメモリカード1300を、ポータブルプレーヤ等の再生装置に挿入することにより、ヘッドフォン等を通じて再生された音楽を楽しむことができる。

【0024】同図に示すように、音楽コンテンツ記録システム1000は、ディスプレイ1191とキーボード1192とを備えるパーソナルコンピュータ1100と、これに挿入されるメモリカードライタ1200とから構成される。パーソナルコンピュータ1100は、CPU、メモリ、ハードディスク等を内蔵し、また、通信回線1001と接続されており、また、いわゆるPCカードスロットであるメモリカードライタ挿入口1195を有する。

【0025】メモリカードライタ1200は、いわゆるPCカードであり、メモリカードを挿入するためのメモリカード挿入口1299を有している。図5は、メモリカードライタ1200の機能ブロック図である。なお、同図には、メモリカード1300の機能ブロックをも示している。パーソナルコンピュータ1100は、通信回線から音楽コンテンツをダウンロードし、特定の音楽コンテンツをメモリカード1300の所定パスに記録すべき指示をメモリカードライタ1200に与えるが、メモリカードライタ1200はこれを受けて、パーソナルコンピュータ1100から暗号化された特定の音楽コンテンツを取り込み、音楽コンテンツを復号して、更に媒体記録用の暗号化等を施してメモリカード1300に記録する機能を有する。特定の音楽コンテンツは、例えば、1曲の音楽コンテンツであり、所定パスとは、ファイルを格納するディレクトリ及びファイル名をいう。

【0026】上記機能を実現するために、メモリカードライタ1200は、ハードウェアとしては認証回路、WM抽出回路、メモリカードインタフェース回路、メモリ、CPU等を備えるものであり、機能的には、ネットワーク上での流通の安全性を確保するために暗号化されている音楽コンテンツを復号するコンテンツ復号部1201と、音楽コンテンツに埋め込まれているCGMSのためのWMを、2ビットデータとして抽出するWM抽出部1202と、音楽コンテンツのメモリカード1300への記録を行う記録部1210とを備える。

【0027】記録部1210は、メカ毎に固有な暗号化用の鍵であるマスタキー1211を記憶しており、認証部1212と、メディア固有キー格納部1213と、ファイルキー生成部1214と、ファイルキー・WM暗号化部1215と、コンテンツ暗号化部1216と、論理アクセス制御部1221及び物理アクセス制御部1222を含むファイルシステム1220とを有する。

【0028】認証部1212は、メモリカード1300と相互認証を行うものであり、マスタキー1211を用いた相互認証の過程において、メモリカード1300に

固有な値であるメディア固有キーを得て、メモリの一領域であるメディア固有キー格納部1213に格納する。なお、ここで相互認証とは、メモリカードとそれに対するアクセス装置の双方の正当性を互いに認証することという。

【0029】ファイルキー生成部1214は、1曲の音楽コンテンツの暗号化用の鍵データである56ビットのファイルキーを乱数等に基づき生成するものであり、コンテンツ暗号化部1216は、コンテンツ復号部1201により復号された音楽コンテンツをファイルキーを用いて暗号化して論理アクセス制御部1221に出力するものであり、ファイルキー・WM暗号化部1215は、ファイルキー生成部1214により生成されたファイルキーと、WM抽出部1202により抽出されたWMとを、メディア固有キー格納部1213に格納されたメディア固有キーを用いてそれぞれDESアルゴリズムにより暗号化し、それぞれ64ビットのデータとして論理アクセス制御部1221に出力するものである。

【0030】論理アクセス制御部1221は、図1、図2に示した論理フォーマットによりメモリカード1300に、コンテンツ暗号化部1216により出力された暗号化された音楽コンテンツをファイル単位の手データとして記録し、ファイルキー・WM暗号化部1215により出力された暗号化ファイルキー及び暗号化WMをファイルエントリの一部として記録するように物理アクセス制御部1222にアクセス指示を行うものである。

【0031】また、物理アクセス制御部1222は、論理アクセス制御部1221によるアクセス指示を受けて、メモリカード1300においてフラッシュメモリ1330のアクセス制御を司るアクセス制御部1320に対して、ブロック単位で、ブロックアドレスを指定しデータ読み出し又は書き込みを指示するものである。なお、ブロックは、フラッシュメモリ1330における物理的なアクセス単位であり、サイズは2048バイトである。

【0032】一方、メモリカード1300は、メモリカードライタ1200等のメモリカードへのアクセス装置との相互認証を行うための認証部1310と、データを記憶可能なフラッシュメモリ1330と、フラッシュメモリ1330の制御を行うアクセス制御部1320とを備える。なお、図6は、メモリカード1300の内部構成を示した図である。同図には、メモリカード1300を構造面に着目して表してあり、同図中の認証IN、認証OUT、CLOCK、ADDRESS IN、DATA IN/OUTは外部ピンであり、当該メモリカードへのアクセス装置との接点となる。

【0033】認証部1310は、メーカ等に固有なマスターキーと、媒体固有のメディア固有キー1312とをユーザがアクセスできない部分に記憶しており、これらを用いてチャレンジレスポンス手順によりメモリカードラ

イタ等と相互認証を行う。相互認証の過程において、認証部1310は、マスターキーを用いて暗号化したメディア固有キー（以下、暗号化メディア固有キーという。）をメモリカードライタ1200の認証部1212に送信し、メモリカードライタ1200の認証部1212は、暗号化メディア固有キーをマスターキー1211を用いて復号してメディア固有キー格納部1213に格納する。

【0034】アクセス制御部1320は、外部とはデータをシリアル転送し、フラッシュメモリ1330とはパラレル転送を行うものであり、メモリカードライタ1200の物理アクセス制御部1222からあるブロックアドレスが指定されブロック単位でシリアルデータが送られた場合に、シリアルデータをパラレル変換してフラッシュメモリ1330内の当該ブロックアドレスで示される位置に書き込む。

【0035】＜2-2. データの記録動作＞以下、メモリカードライタ1200によりなされるメモリカード1300への音楽コンテンツの記録処理について説明する。図7は、メモリカード1300への音楽コンテンツの記録についての処理の流れ及び参照データを示す図である。

【0036】同図に示すように、メモリカード1300への音楽コンテンツの記録は、認証及びメディア固有キー復号処理ステップS1510と、ファイルキー生成処理ステップS1520と、WMの抽出とファイルキー及びWMの暗号化処理ステップS1530と、記録処理ステップS1540とにより実現される。ここで記録処理ステップS1540は、ファイルエントリ書込処理ステップS1541と、コンテンツの暗号化及び書込処理ステップS1542とからなる。

【0037】パーソナルコンピュータ1100から特定の音楽コンテンツの記録指示を受けたメモリカードライタ1200は、認証部1212により、メモリカード1300の認証部1310との間で相互認証を行い、メモリカード1300から暗号化メディア固有キー1391を得て、マスターキー1211を用いてこれを復号した結果であるメディア固有キー1601をメディア固有キー格納部1213に格納する（ステップS1510）。

【0038】認証及びメディア固有キー復号処理ステップS1510の後、ファイルキー生成部1214は、乱数に基づいてファイルキー1602を生成する（ステップS1520）。ファイルキー1602が生成された後、ファイルキー・WM暗号化部1215は、WM抽出部1202により音楽コンテンツから抽出されたWMと、ファイルキー1602とを、メディア固有キー1601を用いて暗号化して、暗号化ファイルキー1603と暗号化WM1604とを生成する（ステップS1530）。

【0039】暗号化ファイルキー1603及び暗号化WM1604の生成後、メモリカードライタ1200は、

ファイルシステム1220を用いて、パーソナルコンピュータ1100に指示されたバス情報に従って、暗号化ファイルキー1603及び暗号化WM1604を含むファイルエントリをメモリカード1300のフラッシュメモリ1330に書き込み(ステップS1541)、また、コンテンツ暗号化部1216により、コンテンツ復号部1201から出力されるコンテンツをファイルキー1602を用いて暗号化して、フラッシュメモリ1330に書き込む(ステップS1542)。

【0040】ファイルエントリ書込処理ステップS1541において、メモリカードドライタ1200は、ファイルシステム1220の論理アクセス制御部1221に対して、図2に示すフォーマットとなるように、暗号化ファイルキー1603と、暗号化WM1604とを格納し、暗号化属性領域長フィールドの値として16を格納する。なお、記録処理ステップS1540においてファイルエントリ内のその他の情報は所定の規則に従って生成、更新する。例えば、Allocation Descriptors [] フィールドには、暗号化した音楽コンテンツを配置したブロックアドレスを格納する。また、ファイルエントリ書き込みに際して、ファイル名やファイルエントリの配置を示す情報等を設定したファイル識別記述子をディレクトリデータへ追加格納する。

【0041】このようにして、メモリカード1300のフラッシュメモリ1330には、図1に示すようなデータ構造で音楽コンテンツであるデータが格納されることになる。

<3. メモリカードプレーヤ>以下、上述した音楽コンテンツ記録システムによりメモリカードに記録された音楽コンテンツを、読み出して音楽を再生するメモリカードプレーヤについて説明する。

【0042】<3-1. 構成>図8は、メモリカードプレーヤの外観図である。同図に示すメモリカードプレーヤ2000は、2枚のメモリカードを挿入可能であり、メモリカードに記録された音楽コンテンツの再生と、音楽コンテンツのコピー、移動等の編集が可能な携帯型の装置であり、液晶表示部2001と、操作ボタン2002と、メモリカード挿入口2011、2012とを備え、ヘッドホン2020が接続されるものである。

【0043】ユーザは、液晶表示部2001に表示されるユーザインタフェース表示を参照しながら操作ボタン2002を操作することにより再生又は編集指示を行うことができ、液晶表示部2001に表示される曲名等を見ながらヘッドホン2020から出力される音楽を聴くことができる。図9は、メモリカードプレーヤ2000の機能ブロック図である。

【0044】なお、同図には、メモリカード1300の機能ブロックをも示している。メモリカードプレーヤ2000は、ハードウェア的には、認証回路、メモリカードインタフェース回路、D/Aコンバータ、メモリ、C

PU等を備えるものであり、機能的には、マスタキー2101を記憶し、認証部2102と、メディア固有キー格納部2103と、ファイルキー・WM復号部2110と、コンテンツ復号部2111と、WM格納部2112と、削除用暗号化部2120と、コピー用処理部2130と、論理アクセス制御部2141及び物理アクセス制御部2142を含むファイルシステム2140と、再生部2150とを備える。

【0045】マスタキー2101、認証部2102及びメディア固有キー格納部2103は、メモリカードドライタ1200におけるマスタキー1211、認証部1212及びメディア固有キー格納部1213と機能的に同等であるため、ここでは説明を省略する。ファイルキー・WM復号部2110は、論理アクセス制御部2141によりメモリカード1300のフラッシュメモリ1330中のファイルエントリが読み出され、ファイルエントリ中の暗号化ファイルキー及び暗号化WMを与えられると、認証部2102によりメディア固有キー格納部2103に格納されているメディア固有キーを用いて、これらを復号してファイルキーをコンテンツ復号部2111又はコピー用処理部と削除用暗号化部2120に出力し、WMをメモリの一領域であるWM格納部2112に出力する。なお、メモリカードプレーヤはユーザ操作を受けて、音楽コンテンツの再生が必要な場合にはファイルキー・WM復号部2110にファイルキーをコンテンツ復号部2111に出力させ、メモリカード中の音楽コンテンツのコピー又は移動が必要な場合にファイルキーをコピー用処理部2130に出力し、移動又は削除が必要な場合にファイルキーを削除用暗号化部2120に出力する。

【0046】コンテンツ復号部2111は、論理アクセス制御部2141によりフラッシュメモリ1330中のファイルである暗号化された音楽コンテンツが読み出されて与えられると、ファイルキー・WM復号部2110により出力されたファイルキーを用いて、暗号化された音楽コンテンツを復号して、再生部2150に出力する。

【0047】再生部2150は、D/Aコンバータ等により実現され、音楽コンテンツをヘッドホン入力用の音声信号に変換して出力する。論理アクセス制御部2141は、図1、図2に示した論理フォーマットでデータが記録されているメモリカード1300から、ファイルエントリ、ファイルであるデータ等を読み出すように、物理アクセス制御部2142にアクセス指示を行うものである。

【0048】物理アクセス制御部2142は、論理アクセス制御部2141によるアクセス指示を受けて、メモリカード1300においてフラッシュメモリ1330のアクセス制御を司るアクセス制御部1320に対して、ブロック単位で、ブロックアドレスを指定しデータ読み

出し又は書き込みを指示するものである。削除用暗号化部2120は、メモリカード内に記録されている音楽コンテンツのファイルを削除する場合又は移動に伴い移動元ファイルの削除をする際に、ファイルキーをメディア固有キーではない他の何らかのキーを用いて暗号化するものであり、これにより得られた暗号化ファイルキーを、論理アクセス制御部2141を介してファイルエントリの暗号化ファイルキーフィールドに書き込むものである。

【0049】コピー用処理部2130は、WM格納部2112に格納されているWMを参照し、音楽コンテンツのコピー可否の判断を行い、必要に応じてWMの値を変更した後にメディア固有キーを用いて暗号化して暗号化WMを生成して、論理アクセス制御部2141を介して暗号化WMをコピー先のファイルエントリの暗号化WMフィールドの値として記録するものである。

【0050】<3-2. データの再生>以下、メモリカードプレーヤ2000によりなされるメモリカード1300に記録された音楽コンテンツの再生処理について説明する。図10は、メモリカード1300に記録された音楽コンテンツの再生についての処理の流れ及び参照データを示す図である。

【0051】同図に示すように、メモリカード1300にファイルとして記録されたデータである暗号化された音楽コンテンツについての再生は、認証及びメディア固有キー復号処理ステップS2510と、ファイルエントリ読出処理ステップS2520と、ファイルキー復号処理ステップS2530と、データの読出及び復号とコンテンツの再生処理ステップS2540とにより実現される。

【0052】ユーザにより特定のファイルの再生指示を受けたメモリカードプレーヤ2000は、認証部2102により、メモリカード1300の認証部1310との間で相互認証を行い、メモリカード1300から暗号化メディア固有キー1391を得て、マスタキー2101を用いてこれを復号した結果であるメディア固有キー2601をメディア固有キー格納部2103に格納する(ステップS2510)。

【0053】認証及びメディア固有キー復号処理ステップS2510の後、メモリカードプレーヤ2000は、ファイルシステム2140を介して、フラッシュメモリ1330内のユーザにより再生指示されたファイルと対となるファイルエントリを読み出す(ステップS2520)。ここで、読み出したファイルエントリ中に暗号化ファイルキー2602が含まれている。なお、ファイルエントリの読み出しの際には、その配置を示すファイル識別記述子を参照する。例えば、図1に示すファイルエントリ130を読み出すためには、ファイルセット記述子103、ルートディレクトリのファイルエントリ110、ファイル識別記述子122に順次アクセスする必要

がある。

【0054】ファイルエントリの読み出しの後、メモリカードプレーヤ2000は、ファイルキー・WM復号部2110により、暗号化ファイルキー2602をメディア固有キー2601を用いて復号して、ファイルキー2603を生成する(ステップS2530)。これによりファイルキー2603はコンテンツ復号部2111に出力される。ステップS2530においては、ファイルエントリ中の暗号化属性領域長フィールドの内容が16であることを確認し、16である場合に暗号化ファイルキーフィールドの暗号化ファイルキーを参照することになる。なお、暗号化属性領域長フィールドの内容が16でない場合には、暗号化フィールドの内容は無効であり、この場合には、ファイルエントリと対となるファイルの内容は暗号化されていない。例えば、曲名や演奏者のリストを示すデータが格納されたファイルは暗号化されていない。

【0055】ファイルキー2603の生成の後、メモリカードプレーヤ2000は、ファイルエントリのAllocation Descriptors フィールドを参照してファイルシステム2140を介して暗号化された音楽コンテンツであるデータをフラッシュメモリ1330から読み出してコンテンツ復号部2111に入力し、ファイルキー2603を用いてコンテンツ復号部2111により復号させて、生の音楽コンテンツ2604を得て再生部2150に送る(ステップS2540)。

【0056】このようにして、メモリカード1300のフラッシュメモリ1330には、図1に示すようなデータ構造で記録されている音楽コンテンツは、再生されることになる。

<3-3. データのコピー>以下、メモリカードプレーヤ2000によりなされるメモリカード1300にファイルとして記録されたデータ、即ち暗号化された音楽コンテンツのメモリカード1400へのコピー処理について説明する。

【0057】図11は、メモリカード1300からメモリカード1400へのデータのコピーについての処理の流れ及び参照データを示す図である。同図に示すように、メモリカード1300からメモリカード1400へのファイルのコピーは、認証及びメディア固有キー復号処理ステップS3010と、ファイルエントリ読出処理ステップS3020と、ファイルキー・WM復号処理ステップS3030と、WMチェック、ファイルキー・WMの暗号化及びファイルエントリとデータのコピー処理ステップS3040とにより実現される。

【0058】ユーザによりメモリカード1300中の特定のファイルをメモリカード1400中の特定パスにコピーすべき旨のコピー指示を受けたメモリカードプレーヤ2000は、認証部2102により、メモリカード1300の認証部1310との間で相互認証を行い、メモ

リカード1300から暗号化メディア固有キー1391を得て、マスタキー2101を用いてこれを復号した結果であるメディア固有キー3101をメディア固有キー格納部2103に格納し、また、メモリカード1400の認証部1410との間でも相互認証を行い、同様にメモリカード1400のメディア固有キー3105をもメディア固有キー格納部2103に格納する(ステップS3010)。

【0059】認証及びメディア固有キー復号処理ステップS3010の後、メモリカードプレーヤ2000は、ファイルシステム2140を介して、フラッシュメモリ1330内のユーザにより指定されたコピー元ファイルと対となるファイルエントリを読み出す(ステップS3020)。なお、読み出したファイルエントリ3102中には図2に示したように、暗号化ファイルキー及び暗号化WMが含まれている。

【0060】ファイルエントリの読み出しの後、メモリカードプレーヤ2000は、ファイルキー・WM復号部2110により、ファイルエントリ3102に含まれる暗号化ファイルキー及び暗号化WMをメモリカード1300のメディア固有キー3101を用いて復号して、復号の結果として得られるWM3103をWM格納部2112に格納し、復号の結果としてえられるファイルキー3104をコピー用処理部2130に出力する(ステップS3030)。

【0061】WM3103をWM格納部2112に格納した後、メモリカードプレーヤ2000は、コピー用処理部2130により、以下に示すWMチェック、ファイルキー・WMの暗号化及びファイルエントリとデータのコピー処理を行う(ステップS3040)。図12は、WMチェック、ファイルキー・WMの暗号化及びファイルエントリとデータのコピー処理を示すフローチャートである。

【0062】コピー用処理部2130は、WM格納部2112に格納されているWM3103を参照し、WMの値によって処理を振り分ける(ステップS3041)。WM3103が、Freeを示す場合には、ファイルキー3104及びWM3103をコピー先であるメモリカード1400のメディア固有キー3105を用いて暗号化し(ステップS3043)、コピー先となるメモリカード1400のフラッシュメモリ1430にファイルシステム2140によってファイルエントリを作成する(ステップS3044)。このファイルエントリの作成は、ファイルエントリ3102中の暗号化WMフィールド、暗号化ファイルキーフィールドにステップS3043により暗号化したWM、ファイルキーを書き込み、また他のフィールドに必要な情報を書き込むことにより行われる。ファイルエントリの作成の後、コピー用処理部2130は、ファイルシステム2140を介してコピー元であるメモリカード1300の特定ファイルをコピー先

であるメモリカード1400の特定パスにコピーし、必要に応じてステップS3044により作成したファイルエントリを更新する(ステップS3045)。

【0063】また、ステップS3041において、WM3103がOne Copyを示す場合には、WM3103の値をNo More Copyを示す値に変更し、その後上述したステップS3043～ステップS3045の処理を行う。また、ステップS3041において、WM3103が、Never又はNo More Copyを示す場合には、ステップS3043～ステップS3045の処理をスキップして処理を終了する。

【0064】このようにして、メモリカード1300のフラッシュメモリ1330に格納されていた1つのファイルであるデータは、メモリカード1400のフラッシュメモリ1430にコピーされる。

<3-4. データの移動>以下、メモリカードプレーヤ2000によりなされるメモリカード1300にファイルとして記録されたデータ、即ち暗号化された音楽コンテンツのメモリカード1400への移動処理について説明する。移動は、前述のコピーの後にコピー元のファイルを削除することにより実現される。

【0065】図13は、メモリカード1300からメモリカード1400へのデータの移動についての処理の流れ及び参照データを示す図である。なお、同図において、前述のメモリカード1300からメモリカード1400へのデータのコピーの処理の場合と同等なものについては、図11におけるそれと同一の符号を付している。

【0066】同図に示すように、メモリカード1300からメモリカード1400へのファイルの移動は、認証及びメディア固有キー復号処理ステップS3010と、ファイルエントリ読出処理ステップS3020と、ファイルキー・WM復号処理ステップS3030と、WMチェック、ファイルキー・WMの暗号化及びファイルエントリとデータのコピー処理ステップS3040と、ファイルキー暗号化及び更新処理ステップS3550とにより実現される。

【0067】ユーザによりメモリカード1300中の特定のファイルをメモリカード1400中の特定パスに移動すべき旨の移動指示を受けたメモリカードプレーヤ2000は、認証部2102により、メモリカード1300の認証部1310との間で相互認証を行い、メモリカード1300から暗号化メディア固有キー1391を得て、マスタキー2101を用いてこれを復号した結果であるメディア固有キー3101をメディア固有キー格納部2103に格納し、また、メモリカード1400の認証部1410との間でも相互認証を行い、同様にメモリカード1400のメディア固有キー3105をもメディア固有キー格納部2103に格納する(ステップS3010)。

【0068】認証及びメディア固有キー復号処理ステップS3010の後、メモリカードプレーヤ2000は、ファイルシステム2140を介して、フラッシュメモリ1330内のユーザにより指定されたコピー元ファイルと対となるファイルエントリを読み出す（ステップS3020）。なお、読み出したファイルエントリ3102中には図2に示したように、暗号化ファイルキー及び暗号化WMが含まれている。

【0069】ファイルエントリの読み出しの後、メモリカードプレーヤ2000は、ファイルキー・WM復号部2110により、ファイルエントリ3102に含まれる暗号化WMをメモリカード1300のメディア固有キー3101を用いて復号して、復号の結果として得られるWM3103をWM格納部2112に格納し、暗号化ファイルキーをメモリカード1300のメディア固有キー3101を用いて復号しファイルキー3104を得る（ステップS3030）。

【0070】WM3103及びファイルキー3104を生成した後、メモリカードプレーヤ2000は、コピー用処理部2130により、WMチェック、ファイルキー・WMの暗号化及びファイルエントリとデータのコピー処理を行い（ステップS3040）、削除用暗号化部2120により、ファイルキー3104をメディア固有キー以外のキーを用いて暗号化して、その結果得られる暗号化ファイルキーを、ファイルシステム2140により移動元のファイルについてのファイルエントリの暗号化ファイルキーフィールドに書き込み、また当該ファイルエントリを指し示すファイル識別子（図1、図3参照）のFileCharacteristicsフィールドを削除済みであることを示すように更新する（ステップS3550）。

【0071】このようにして、メモリカード1300のフラッシュメモリ1330に格納されていた1つのファイルであるデータは、メモリカード1400のフラッシュメモリ1430にコピーされ、コピー元のファイルについては削除される。なお、削除されたファイルについてのファイルエントリ中の暗号化ファイルキーを、メディア固有キー以外のキーにより暗号化するのは、削除ファイルを何らかの方法で復活させても、そのファイルの内容である音楽コンテンツを再生することができないようにするためである。

<実施の形態2>以下、本発明の実施の形態2に係るデジタル著作物記録媒体（フラッシュメモリ）の論理的データ構造について説明する。実施の形態2に係るフラッシュメモリの論理的データ構造は、UDFを採用し、ファイルエントリ内の拡張属性領域を利用して、暗号化フラグフィールド、暗号化ファイルキーフィールド、暗号化WMフィールドを定義したものである。従って、ファイルエントリ以外については、実施の形態1と同様の論理的データ構造である（図1、図3参照）。

【0072】図14は、実施の形態2に係るファイルエントリのデータ構造を示す図である。同図中、実施の形態1に係るファイルエントリと同一内容のフィールドについては、同一符号を付してあり、その説明は省略する。拡張属性を示す情報を複数格納できるフィールドであるExtendedAttributes [] フィールド213は、DescriptorTagフィールド5101と、ImplementationAttributesLocationフィールド5102と、ApplicationAttributesLocationフィールド5103と、ImplementationUseExtendedAttributeフィールド5104、5105等と、ApplicationUseExtendedAttributeフィールド5106、5107等とからなる。

【0073】ここで、DescriptorTagフィールド5101は、拡張属性の識別子を示す固定値を格納する16バイトのフィールドである。ImplementationUseExtendedAttributeフィールド5104、5105等は、それぞれシステムが使用可能な拡張属性を格納する可変長のフィールドであり、その先頭位置が、ImplementationAttributesLocationフィールド5102に格納される。

【0074】また、ApplicationUseExtendedAttributeフィールド5106、5107等は、それぞれユーザが使用可能な拡張属性を格納する可変長のフィールドであり、その先頭位置が、ApplicationAttributesLocationフィールド5103に格納される。同図には、ImplementationUseExtendedAttribute5105が、ファイルについての暗号化に用いられた鍵や電子透かし等に関する拡張属性のフィールド（以下、暗号情報フィールドという。）である例を示しており、当該暗号情報フィールドはさらに、AttributeTypeフィールド5201と、AttributeSubTypeフィールド5202と、Reservedフィールド5203と、AttributeLengthフィールド5204と、ImplementationUseLengthフィールド5205と、ImplementationIdentifierフィールド5206と、HeaderChecksumフィールド5207と、暗号化フラグフィールド5208と、Reservedフィールド5209と、暗号化ファイルキーフィールド5210と、暗号化WMフィールド5211とで構成される。

【0075】AttributeTypeフィールド5201とAttributeSubTypeフィールド5202は、拡張属性の種別、サブ種別が格納されるフィールドであり、同図の例では、暗号情報フィールドで

あることを示す固定値、例えばそれぞれ1000、10が格納される。Reservedフィールド5203、5209は、将来の機能拡張等のための予備的領域である。

【0076】AttributeLengthフィールド5204は、拡張属性のサイズを格納するフィールドであり、その内容は、暗号情報フィールドについては68となる。ImplementationUseLengthフィールド5205は、ImplementationIdentifierフィールドに続く全フィールドのサイズを格納するフィールドであり、その内容は、暗号情報フィールドについては20となる。

【0077】ImplementationIdentifierフィールド5206は、拡張属性の識別子を格納するフィールドであり、暗号情報フィールドについては例えば、“*Flash Crypto Info”となる。暗号化フラグフィールド5208は、暗号化ファイルキーフィールド5210及び暗号化WMフィールド5211が有効であるか否かを示す情報を格納するフィールドであり、最上位ビットが1であれば有効を示し、実施の形態1における暗号化属性領域長フィールドの値が16であることと同様に扱われる。

【0078】暗号化ファイルキーフィールド5210及び暗号化WMフィールド5211については、実施の形態1における暗号化ファイルキーフィールド211及び暗号化WMフィールド212と内容的に同等である。また、HeaderChecksumフィールド5207は、暗号化フラグフィールド5208から暗号化WMフィールド5211までに格納された値のチェックサムを格納するフィールドである。

【0079】なお、ファイルエントリ内の暗号化ファイルキー及び暗号化WMの参照又は更新、ファイルの記録、読み出し等のフラッシュメモリへのアクセスについては、実施の形態1で説明したデータの記録、再生、複製、移動の処理と基本的に同様の処理により行うことができる。但し、実施の形態2に係るフラッシュメモリについては、データの記録の際には、HeaderChecksumフィールド5207にはチェックサムを算出して格納し、データの読み出しの際には、当該チェックサムを確認することとする。

<実施の形態3>以下、本発明の実施の形態3に係るデジタル著作物記録媒体（フラッシュメモリ）の論理的データ構造について説明する。実施の形態3に係るフラッシュメモリの論理的データ構造は、JIS-X-0605規格に規定されているFAT型の論理フォーマットを採用したものであり、一般的なFAT型のフォーマットにおけるディレクトリ項目の未使用領域を利用して、ファイルの暗号化等に関する情報を格納するものである。

【0080】図15は、実施の形態3に係るディレクト

リ項目のデータ構造を示す図である。ディレクトリ項目6100は、全体で32バイトの大きさをもち、11バイトのファイル名と、ファイルの属性と、記録時間と、記録日付と、先頭クラスタ番号と、ファイル長との各フィールドを含み、さらに本発明の特徴である暗号化フラグフィールド6101と、暗号化されたファイルキー+WMフィールド6102を含む。

【0081】ファイルの属性は、ボリュームラベルビット、サブディレクトリビットを含み、ボリュームラベルビットが1であればディレクトリ項目がボリュームラベルについてのものであることを示し、サブディレクトリビットが1であればディレクトリ項目がサブディレクトリについてのものであることを示し、いずれもが0であれば、ディレクトリ項目がファイルに対応するものであることを示す。

【0082】暗号化フラグフィールド6101は、ディレクトリ項目6100の先頭を0バイト目とすると13バイト目に位置する1バイト（8ビット）中の下位1ビットで、暗号化されたファイルキー+WMフィールド6102の内容が有効であるか否かを示すフィールドであり、当該1ビットが1であれば有効、0であれば無効を意味する。

【0083】暗号化されたファイルキー+WMフィールド6102は、ディレクトリ項目6100の14バイト目から21バイト目までの8バイト（64ビット）のフィールドであり、実施の形態1で説明した56ビットのファイルキーと2ビットのWMとを合成して、メディア固有キーを用いてDESアルゴリズムにより暗号化して得られる64ビットデータ、即ち暗号化されたファイルキー+WMを格納するフィールドである。

【0084】フラッシュメモリへのアクセスについては、暗号化の鍵及びWM等に関連する情報が実施の形態1におけるファイルエントリから、ディレクトリ項目に変更されただけであるため、基本的には実施の形態1に示したアクセス制御を行うものである。即ち、フラッシュメモリに、音楽コンテンツを暗号化してファイルとして記録する場合には、当該ファイルに対応するディレクトリ項目に、音楽コンテンツに埋め込まれたWMと暗号化に用いたファイルキーとを合成してメディア固有キーで暗号化したものである暗号化されたファイルキー+WMを格納した上で暗号化フラグフィールド6101の内容を1にする。

【0085】また、フラッシュメモリからのデータの読み出しにおいては、ディレクトリ項目の暗号化フラグフィールド6101の内容が1であり、かつ、ファイルの属性のボリュームラベルビット及びサブディレクトリビットが共に0である場合には、ディレクトリ項目に対応するファイルが暗号化されたファイルであると判断でき、暗号化されたファイルキー+WMフィールドから暗号化されたファイルキー+WMを取り出して、メディア

固有キーを用いて復号することによりファイルキー及びWMを得ることができる。このファイルキーを用いてファイルの内容である音楽コンテンツを復号して再生することや、WMを参照してファイルのコピー等を行うことができる。

【0086】以上、本発明に係るデジタル著作物記録媒体のデータ構造及び当該記録媒体へのアクセス装置について、実施の形態に基づいて説明したが、本発明はこれらの実施の形態に限られないことは勿論である。即ち、

(1) 実施の形態1では、メモ리카ードにオーディオデータを記録するメモ리카ードライタ1200は、PCカードであることとしたが、これに限定されることはなく、据え置き型の装置であってもよいし、また、可搬性のある装置であってもよい。例えば、実施の形態1に示したメモ리카ードプレーヤに、メモ리카ードライタとしての機能を併せ持たせてもよい。

【0087】また、メモ리카ードライタ内に示したコンテンツ復号部等の一部機能はパーソナルコンピュータ側にあってもよく、メモ리카ードライタの全機能をパーソナルコンピュータ側にソフトウェアを用いて実現することとしてもよい。

(2) 実施の形態1では、ファイルキー生成部1214は、乱数に基づいてファイルキーを生成することとしたが、ある程度ファイル毎に異なるファイルキーが生成できる方法によれば乱数に基づいて生成する必要はない。また、ファイルキー生成部1214は、乱数の種をメモ리카ードから受け取って、これにより発生する乱数に基づいてファイルキーを生成することとしてもよい。

(3) 実施の形態1では、メモ리카ードライタ1200は、メディア固有キーを用いてファイルキーを暗号化することとしたが、これに限定されることはなく、ユーザからパスワードを受け付けて、当該パスワードを用いてメディア固有キーを変換した上で、変換後のメディア固有キーを用いてファイルキーを暗号化することとしてもよい。この場合には、メモ리카ードプレーヤにおいてユーザからパスワードを受け付けて、当該パスワードを用いてメディア固有キーを変換した上で、変換後のメディア固有キーを用いて暗号化ファイルキーを復号すればよい。

【0088】また、実施の形態1におけるマスターキーに加えて、マスターキー配下の細分化した単位固有の暗号化用の鍵であるサブグループキーをも用いることとしてもよく、この場合、メディア固有キーは、メモ리카ードの認証部によりサブグループキーを用いて変換された後にマスターキーを用いて暗号化されて暗号化メディア固有キーとして、メモ리카ードライタ又はメモ리카ードプレーヤ等のメモ리카ードアクセス装置に認証の際に与えられることとしてもよく、これに対応してメモ리카ードアクセス装置は暗号化メディア固有キーをマスターキーを用い

て復号した後にサブグループキーを用いて逆変換することによりメディア固有キーを得ることとしてもよい。

【0089】また、メディア固有キーはマスターキーを用いて暗号化された後にサブグループキーを用いて変換されてメモ리카ードの認証部から認証の過程で送信されることとしてもよく、また、メディア固有キーは、サブグループキーを用いて変換された後のマスターキーを用いて暗号化されてメモ리카ードの認証部から認証の過程で送信されることとしてもよい。この場合にも、これらに対してメモ리카ードアクセス装置は、逆変換及び復号を行うことによりメディア固有キーを得ることとすればよい。

【0090】さらに、ファイルキーの暗号化に用いるキーは、サブグループキーであることとしても、サブグループキーとメディア固有キーの組合せであることとしてもよい。

(4) 実施の形態1、2では、WMはメディア固有キーを用いて暗号化され、ファイルエントリの暗号化WMフィールドに格納されることとしたが、メディア固有キー以外の鍵を用いて暗号化されることとしてもよい。例えば、ファイルキーを用いてWMが暗号化されることとしてもよい。また、暗号化ファイルキーフィールドと暗号化WMフィールドに格納される暗号化ファイルキーと暗号化WMとはそれぞれ別の鍵を用いて暗号化されることとしてもよい。また、WMは暗号化されずに暗号化WMフィールドに格納されることとしてもよい。

【0091】また、実施の形態1、2における暗号化ファイルキーフィールドと暗号化WMフィールドとは、実施の形態3における暗号化されたファイルキー+WMフィールドのように一体化してもよい。即ち、ファイルキーとWMとを所定の規則に基づいて混合した後に、メディア固有キーを用いて暗号化して、一体化したフィールドに格納することとしてもよい。

(5) 実施の形態1～3では、WMは、2ビットのCGMSとしたが、これに限定されることはなく、ファイルの内容として埋め込まれている電子透かしであれば、著作権者名や所有者名等を意味するデータであってもよく、何ビットのデータであってもよい。但し、実施の形態3に示したようなFAT型のフォーマットをそのまま採用する場合には、暗号化されたファイルキー+WMが、ディレクトリ項目の未使用領域内に収まるように、WMのデータサイズが制限される。

(6) 実施の形態1～3においてファイルキー及びWMの暗号化アルゴリズムはDESアルゴリズムとしたが、これに限定されることはなく、DES以外のブロック暗号化アルゴリズムを用いることとしてもよい。

【0092】また、ファイルキーのビット数も56ビットに限定されない。従って、実施の形態1、2に示した暗号化ファイルキーフィールド及び暗号化WMフィールドのサイズは、特に8バイトに限定されることはない。

また、実施の形態2、3で示した暗号化フラグのビット位置は、どの位置であってもよい。

(7) 実施の形態1～3では、ファイルキー及びWMが暗号化されて、ファイルに対応するファイルエントリ又はディレクトリ項目に含まれることとしたが、ファイルキー又はWMの一方が存在しないこととしてもよい。即ち、WMに関連する情報はファイルエントリ又はディレクトリ項目に含ませないこととしてもよいし、ファイル内容は暗号化せずにファイルキーに関連する情報はファイルエントリ又はディレクトリ項目に含ませないこととしてもよい。これらの場合、一方のみの存在の有無を暗号化属性領域長フィールド又は暗号化フラグフィールドの内容が示すこととすればよい。

(8) 実施の形態1～3では、メモ리카ードのフラッシュメモリに記録されるデータの論理的データ構造を示したが、この論理的データ構造は、メモ리카ード以外の他の記録媒体においても適用できるものである。また、ファイルとして記録されるべきデータは、音楽コンテンツに限定されず、他のデジタル著作物であってもよく、記録媒体中にデジタル著作物のファイルと、その他の管理情報等のファイルとが混在してもよい。

(9) 実施の形態1では、ファイルを格納するディレクトリ位置やファイル名を示すバス情報はパーソナルコンピュータからメモ리카ードライタに指示するものとしたが、メモ리카ードライタがファイル名やファイル格納位置を決定することとしてもよい。

(10) 実施の形態1では、1曲の音楽コンテンツが1つのファイルに格納されることとしたが、1曲より小さな単位がコピー、流通等の取り扱い単位である場合には、1曲より小さい単位を1ファイルとしてもよく、また、逆に、1曲より大きい単位を1ファイルとしてもよく、1ファイルの内容は、曲の概念に拘束されない。

(11) 実施の形態1では、データの移動処理について説明したが、データの削除についても、データ移動処理の一部と同様に、ファイルキーは、復号不可能なもの、即ち他の鍵によって暗号化されたものに更新される。なお、削除されたファイルは、例えばごみ箱的なディレクトリに移されることとしてもよい。また、移動及び削除の際に、ファイルキーのみならずWMをもメディア固有キー以外の鍵によって暗号化することとしてもよい。

【0093】なお、移動にともなう削除のためにファイルキー又はWMを暗号化するとき、移動先のメディア固有キーをその暗号化の鍵として用いることとしてもよい。これにより、削除ファイルを復活するには、移動先の記録媒体が必要になるため、復活時には移動先のファイルの存在を確認して削除した移動元のファイルを復活させるとともに移動先のファイルを削除するという機能、即ち不正コピーを防止した削除ファイル復活機能が実現できる。

(12) 実施の形態1、2では、フラッシュメモリの1

ブロックのサイズが2048バイトとしたが、これに限定されることはなく、512バイト等の一定サイズであればよい。

(13) 実施の形態1では、メモ리카ードライタ等のアクセス装置とメモ리카ードとの間でシリアル転送によりデータ送受を行うこととしたが、例えば16ビットパラレルの転送であってもよい。この場合、アクセス制御部1320はメモ리카ード1300とアクセス装置間の16ビットパラレルのデータをフラッシュメモリのデータビット幅である8ビットに変換を行う等のバス幅の変換や信号レベルの変換を行う。

【0094】また、アクセス装置とメモ리카ードとの接続は、Universal Serial Bus (USB) 等の汎用のシリアルバスを用いてもよいし、メモ리카ード1300がUSBのコネクタに直接差し込めてもよく、また、カード挿入口にUSBデバイスが挿入可能ないようにしてUSBカメラやUSBキーボードなどのUSB周辺機器と混在利用ができるようにしてもよい。

【0095】また、シリアルバスとしてイーサネット等のネットワークを用いIPプロトコルで転送を行ってもよい。この場合、メモ리카ードのインタフェース部分ではIPプロトコル制御部等によりIPプロトコル変換を行えばよい。

(14) 実施の形態1～3に示したデータ構造でデータを記録した記録媒体を流通・販売の対象にしても良い。

【0096】また、実施の形態1に示したようなデータ記録、データ再生、データコピー、データ削除の処理内容を実現する機械語プログラムを記録した記録媒体を流通・販売の対象にしてもよい。記録媒体には、ICカード、光ディスク、フレキシブルディスク、ROM等があるが、これらに記録された前記機械語プログラムは、汎用コンピュータやプログラム実行機能を有する家電機器にインストールされることにより利用に供される。即ち、汎用のコンピュータ又はプログラム実行機能を有する家電機器は、インストールした前記機械語プログラムを逐次実行して、実施の形態に示したようなデータ記録等を実現する。なお、上記のデータ記録等の処理内容を実現するための高級言語で記述されたプログラムを、ハードディスク等の記録媒体及び各種通信路等を介して流通させ頒布することもできる。

【0097】

【発明の効果】以上の説明から明らかなように、本発明に係るデジタル著作物記録媒体は、第1鍵を用いて暗号化されたデジタル著作物データをファイルとして記録したコンピュータ読み取り可能なデジタル著作物記録媒体であって、前記ファイルに対応し当該ファイルの記録位置に関する情報を含む管理情報を記録した論理的な領域としての管理情報領域を含み、前記管理情報領域はさらに、前記第1鍵を、第2鍵を用いて暗号化したものである暗号化第1鍵を記録した領域を含むことを特徴

とする。

【0098】これにより、ファイルの内容の暗号化に用いた第1鍵を論理的な領域である管理情報領域に記録するため、記録媒体の物理的構造に依存せず、また、ファイル内容となるコンテンツ等の特有のデータ構造等にも依存せず、第1鍵、即ちファイルキーを暗号化して記録することができる。ここで管理情報領域とは、例えばUDFにおけるファイルエントリであり、通常、ファイルの読み出し装置は、このファイルエントリを参照することにより、ファイルにアクセスするものであるため、ファイルエントリ参照と同時に、ファイルエントリ内に論理的に位置づけられた暗号化されたファイルキーを読み出し可能となる。従って、ファイルの読み出し装置は、暗号化されたファイルキーを復号してファイルキーを得ることにより、ファイルキーを用いてファイル内容を迅速に復号することができる。

【0099】即ち、デジタル著作物のセキュリティを高めるために、ファイル単位に異なる暗号化用の鍵を用いてファイル内容を暗号化した場合に、上記記録形式によれば当該ファイルの復号の迅速化を図ることができることになるため、デジタル著作物を、セキュリティ面と利用面とにおいて最適なデータ構造で記録しているといえる。

【0100】また、前記第2鍵は、暗号化第1鍵とは別の領域に単独で記録されていることとすることもできる。これにより、ファイルキーの暗号化用の鍵は記録媒体中に含まれているため、当該記録媒体にアクセスする装置は、この鍵を取得することにより、ファイルキーを復号することができ、ファイルの内容を復号することもできるようになる。

【0101】また、前記管理情報領域はさらに、前記暗号化第1鍵を記録した領域の内容が有効か否かを示す暗号化有無フラグを記録した領域を含むこととすることもできる。これにより、暗号化されたファイルキーが有効に記録されているかについての情報である暗号化フラグが、例えばファイルエントリ等の形式の管理情報領域中に格納されているため、記録媒体にアクセスする装置は、ファイルにアクセスするために管理情報領域を参照した際に、暗号化フラグを参照することができ、暗号化フラグに基づいて、ファイルが暗号化されているかされていないかを判断することができる。この場合、前記装置は、暗号化フラグが、暗号化されたファイルキーが有効に記録されている旨を示しているときには、当該ファイルの内容は暗号化されているため、前記暗号化されたファイルキーを復号して、これを用いて当該ファイルの内容を復号して利用することができ、暗号化フラグが、暗号化されたファイルキーが有効に記録されていない旨を示しているときには、当該ファイルの内容は暗号化されていないため、当該ファイルの内容をそのまま利用することができる。

【0102】また、本発明に係るデジタル著作物記録媒体は、電子透かしが埋め込まれたデジタル著作物データをファイルとして記録したコンピュータ読み取り可能なデジタル著作物記録媒体であって、前記ファイルに対応し当該ファイルの記録位置に関する情報を含む管理情報を記録した論理的な領域としての管理情報領域を含み、前記管理情報領域はさらに、前記電子透かしを表す情報を記録した領域を含むことを特徴とする。

【0103】これにより、WMが、記録媒体における管理情報領域中に記録されているため、当該記録媒体中のファイルのコピー等を行う装置は、ファイル内容である暗号化されたデジタル著作物データから直接的にWMを抽出する必要なく、容易にWMを参照することができる。WM抽出用の回路は回路規模も大きく、消費電力も高く、抽出に時間がかかるという欠点をもつが、本発明によれば前記装置は、WM抽出用の回路を内蔵する必要がなく、小型軽量化が図れ、また、前記WMがファイルのコピー可否に関する情報を含む場合には、容易に当該WMを参照することができるため迅速なコピー等が可能となる。

【0104】また、前記電子透かしは前記デジタル著作物データのコピー可否に関する情報であり、前記電子透かしを表す情報は、前記電子透かしを、第2鍵を用いて暗号化したものである暗号化電子透かしであることとすることもできる。これにより、WMを暗号化したものを管理情報領域中に記録するため、WMが不正な覗き見から保護され、WMの改ざんの困難性も高まる。また、WMがファイルのコピー可否に関する情報であり管理情報領域中に記録されることから、コピーすべきファイルについての情報を得るために管理情報領域を参照した際に、同時にコピー可否を判断することができるので、ファイルのコピーが迅速に行えるようになる。

【0105】また、本発明に係るデジタル著作物記録媒体は、電子透かしが埋め込まれたデジタル著作物データを、第1鍵を用いて暗号化したものをファイルとして記録したコンピュータ読み取り可能なデジタル著作物記録媒体であって、前記ファイルに対応し当該ファイルの記録位置に関する情報を含む管理情報を記録した論理的な領域としての管理情報領域を含み、前記管理情報領域はさらに、前記第1鍵を、第2鍵を用いて暗号化したものである暗号化第1鍵を記録した領域と、前記電子透かしを前記第1鍵又は前記第2鍵を用いて暗号化したものを記録した領域とを含むことを特徴とする。

【0106】これにより、ファイルの内容の暗号化に用いた第1鍵と、ファイルの内容に埋め込まれているWMとをともに論理的な領域である管理情報領域に記録するため、記録媒体の物理構造に依存せず、また、ファイル内容となるコンテンツ等の特有のデータ構造等にも依存せず、第1鍵及びWMを暗号化して記録することができる。従って、記録媒体にアクセスする装置は、管理情報

領域にアクセスすれば、ファイルの位置情報を得るとともに、暗号化された第1鍵や暗号化されたWMを得ることができるので、ファイル内容の復号等を迅速に行うことができる。

【0107】また、前記管理情報領域は、前記第1鍵と前記電子透かしとを合わせたものを前記第2鍵を用いて暗号化して記録した領域を含むこととすることもできる。これにより、記録媒体の管理情報領域内には、ファイルキーとWMとが混合された上で暗号化されたものが記録されるため、WMの改ざんがなされればファイルキーが破壊されることになり、セキュリティが高まる。

【0108】また、前記デジタル著作物記録媒体はさらに、当該デジタル著作物記録媒体にアクセスする装置との間で相互認証を実行するアクティブ素子を有することとすることもできる。これにより、認証に成功した場合にのみファイルにアクセスされ得るため、セキュリティが高まる。

【0109】また、前記デジタル著作物記録媒体はさらに、当該デジタル著作物記録媒体にアクセスする装置との間で相互認証を実行するアクティブ素子を有し、前記第2鍵は、前記デジタル著作物記録媒体に固有な値の鍵であり、前記相互認証の過程において前記デジタル著作物記録媒体から前記第2鍵を暗号化したものが前記装置に送信されることとすることもできる。

【0110】これにより、認証に成功した装置からのみアクセスされ得るため、セキュリティは高まる。また、記録媒体が、暗号化された第1鍵又は暗号化されたWMの復号のための鍵を認証過程で与えるため、当該記録媒体にアクセスする装置は認証に成功した場合には、第1鍵又はWMを復号できる。また、前記ファイルはUniversal Disk Formatに従って記録されており、前記管理情報領域は、Universal Disk Formatにおけるファイルエントリであり、前記暗号化第1鍵を記録した領域は、前記ファイルエントリ中の拡張属性領域であることとすることもできる。

【0111】これにより、UDF対応のアクセス装置からは、記録媒体内のファイルを操作することができるようになる。また、UDF対応のアクセス装置を機能拡張すれば、暗号化されたファイルの内容を復号する等が行えるようになる。また、前記デジタル著作物記録媒体において前記ファイルはFAT型フォーマットに従って記録されており、前記管理情報領域は、JIS-X-0605規格のFAT型フォーマットにおけるディレクトリ項目であり、前記暗号化第1鍵を記録した領域は、前記ディレクトリ項目中の未使用領域であることとすることもできる。

【0112】これにより、FAT型フォーマット対応のアクセス装置からは、記録媒体内のファイルを操作することができるようになる。また、FAT型フォーマット

対応のアクセス装置を機能拡張すれば、暗号化されたファイルの内容を復号する等が行えるようになる。また、本発明に係る記録装置は、認証機能を有するアクティブ素子を備える記録媒体に、認証成功後に暗号化されたデジタル著作物データをファイルとして記録する記録装置であって、前記記録媒体と相互認証を行う認証手段と、第1鍵を用いて暗号化された前記デジタル著作物をファイルとして前記記録媒体に記録するファイル記録手段と、第2鍵を用いて暗号化された前記第1鍵と、前記ファイルの記録位置に関する情報とを論理的に一体でありかつ当該ファイルに1対1で対応する管理情報領域に含めて、前記記録媒体に記録することを特徴とする。

【0113】これにより、ファイルの内容の暗号化に用いた第1鍵を論理的な連続領域である管理情報領域に記録するため、記録媒体の物理的構造に依存せず、また、ファイル内容となるコンテンツ等の特有のデータ構造等にも依存せず、第1鍵、即ちファイルキーを暗号化して記録することができる。また、本発明に係る再生装置は、認証機能を有するアクティブ素子を備え、かつ、第1鍵を用いて暗号化されたデジタル著作物データがファイルとして記録され、かつ、前記第1鍵が第2鍵を用いて暗号化されたものと当該ファイルの記録位置に関する情報とが論理的な管理情報領域に記録されている記録媒体から、認証成功後に、当該暗号化されたデジタル著作物データを読み出して復号して再生する再生装置であって、前記記録媒体と相互認証を行う認証手段と、前記管理情報領域に記録されている暗号化された前記第1鍵を読み出し、前記第2鍵を用いて復号する第1鍵復号手段と、前記ファイルとして記録されている暗号化されたデジタル著作物データを読み出し、前記第1鍵復号手段により復号された第1鍵を用いて復号して再生するデータ復号再生手段とを備えることを特徴とする。

【0114】これにより、ファイルの位置情報を得るために管理情報領域を参照すると同時に、管理情報領域内に論理的に位置づけられた暗号化されたファイルキーを読み出すことができるため、再生装置は、暗号化されたファイルキーを復号してファイルキーを得ることにより、ファイルキーを用いてファイル内容を迅速に復号し再生することができる。

【0115】また、本発明に係る削除装置は、認証機能を有するアクティブ素子を備え、かつ、第1鍵を用いて暗号化されたデジタル著作物データがファイルとして記録され、かつ、前記第1鍵が第2鍵を用いて暗号化されたものと当該ファイルの記録位置に関する情報と当該ファイルが削除されたものであるか否かを示す削除情報とが論理的な管理情報領域に記録されている記録媒体から、認証成功後に、当該暗号化されたデジタル著作物データを論理的に削除する削除装置であって、前記記録媒体と相互認証を行う認証手段と、前記管理情報領域に記録されている暗号化された前記第1鍵を読み出し、前

記第2鍵を用いて復号して得られる前記第1鍵を前記第2鍵と異なる第3鍵で暗号化して、前記読み出した位置に記録し、前記管理情報領域中の前記削除情報を、ファイルが削除されたものである旨を示すように更新することを特徴とする。

【0116】これにより、管理情報領域の内容の書換えによってファイルを論理的に削除する場合において、暗号化された第1鍵、即ち、暗号化されたファイルキーを、通常暗号化に用いる第2鍵と異なる別の第3鍵を用いて暗号化するものであるため、たとえ管理情報領域の内容の書換えによってファイルを復活させた場合にも、通常の第2鍵を用いた復号手段ではファイルキーが復号できない。従って、例えば、コピーが禁止されているデジタル著作物を内容とするファイルのある記録媒体から別の記録媒体に移動する場合において、コピー後に移動元のファイルを高速に削除するために論理的な削除の方法を用いたときであっても、何らかの操作によって削除されたファイルが復活して、利用できるデジタル著作物の複製が2つ存在するような事態を防止することができる。

【図面の簡単な説明】

【図1】本発明の実施の形態1に係るデジタル著作物記録媒体（フラッシュメモリ）の論理的データ構造を示す図である。

【図2】ファイルエントリのデータ構造を示す図である。

【図3】ファイル識別記述子のデータ構造を示す図である。

【図4】音楽コンテンツ記録システムの外観図である。

【図5】メモ리카ードライタ1200の機能ブロック図である。

【図6】メモ리카ード1300の内部構成を示す図である。

【図7】メモ리카ード1300への音楽コンテンツの記録についての処理の流れ及び参照データを示す図である。

【図8】メモ리카ードプレーヤの外観図である。

【図9】メモ리카ードプレーヤ2000の機能ブロック図である。

【図10】メモ리카ード1300に記録された音楽コンテンツの再生についての処理の流れ及び参照データを示す図である。

【図11】メモ리카ード1300からメモ리카ード1400へのデータのコピーについての処理の流れ及び参照データを示す図である。

【図12】WMチェック、ファイルキー・WMの暗号化及びファイルエントリとデータのコピー処理を示すフローチャートである。

【図13】メモ리카ード1300からメモ리카ード1400へのデータの移動についての処理の流れ及び参照デ

ータを示す図である。

【図14】実施の形態2に係るファイルエントリのデータ構造を示す図である。

【図15】実施の形態3に係るディレクトリ項目のデータ構造を示す図である。

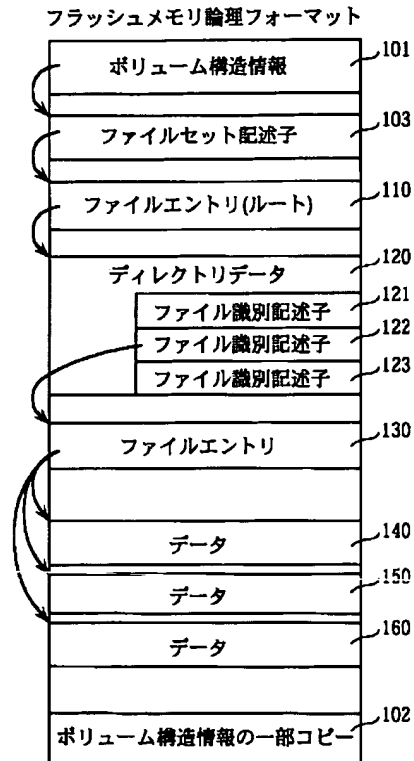
【符号の説明】

101	ボリューム構造情報
102	ボリューム構造情報の一部コピー
103	ファイルセット記述子
121、122、123	ファイル識別記述子
110、130	ファイルエントリ
140、150、160	データ
210	暗号化属性領域長フィールド
211	暗号化ファイルキーフィールド
212	暗号化WMフィールド
1200	メモ리카ードライタ
1201	コンテンツ復号部
1202	WM抽出部
1210	記録部
1211	マスタキー
1212	認証部
1213	メディア固有キー格納部
1214	ファイルキー生成部
1215	WM暗号化部
1216	コンテンツ暗号化部
1220	ファイルシステム
1221	論理アクセス制御部
1222	物理アクセス制御部
1300	メモ리카ード
1310	認証部
1312	メディア固有キー
1320	アクセス制御部
1330	フラッシュメモリ
2000	メモ리카ードプレーヤ
2101	マスタキー
2102	認証部
2103	メディア固有キー格納部
2110	WM復号部
2111	コンテンツ復号部
2112	WM格納部
2120	削除用暗号化部
2130	コピー用処理部
2140	ファイルシステム
2141	論理アクセス制御部
2142	物理アクセス制御部
2150	再生部
5208	暗号化フラグフィールド
5210	暗号化ファイルキーフィールド
5211	暗号化WMフィールド
6100	ディレクトリ項目

- 6101 暗号化フラグフィールド
6102 暗号化されたファイルキー+WMフィールド

ド

【図1】

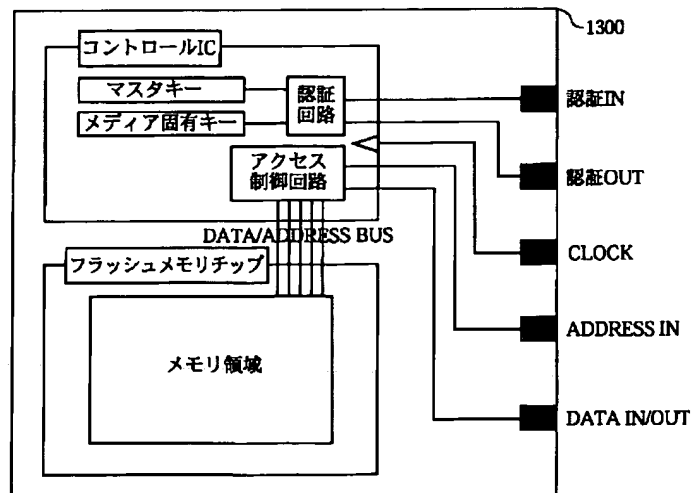


【図2】

ファイルエントリ

フィールド名	長さ
201 DescriptorTag	16
202 ICBTag	20
203 Uid	4
204 Gid	4
..	..
205 AccessTime	12
206 ModificationTime	12
..	..
207 UniqueID	8
208 LengthOfExtendedAttributes	4
209 LengthOfAllocationDescriptors	4
210 暗号化属性領域長	4
211 暗号化ファイルキー	8
212 暗号化WM	8
213 ExtendedAttributes[]	可変長
214 AllocationDescriptors[]	可変長

【図6】

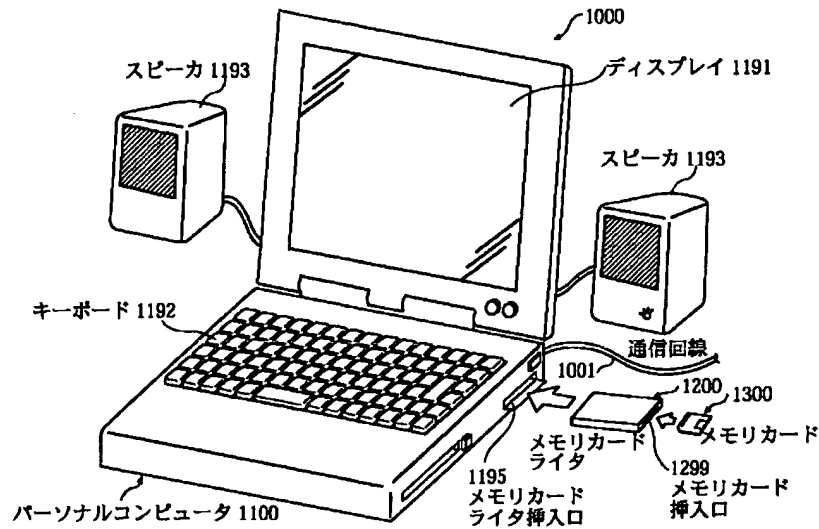


【図3】

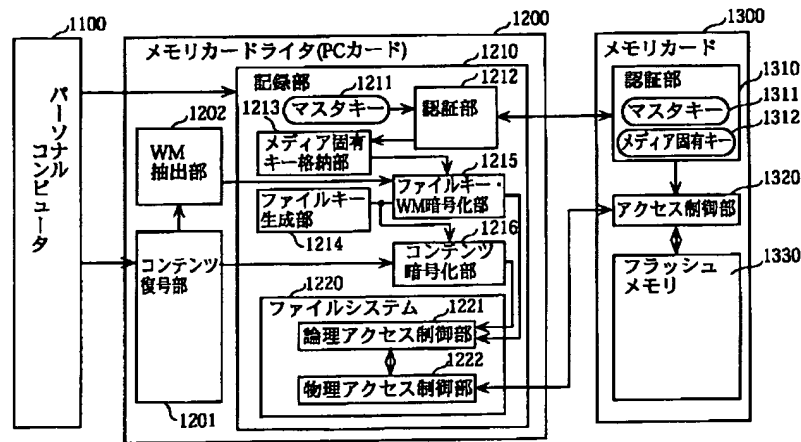
ファイル識別記述子

フィールド名	長さ
DescriptorTag	16
File Version Number	2
301 File Characteristics	1
Length of File Identifier	2
302 ICB	16
Length of Implementation	2
Implementation Use	可変長
303 File Identifier	可変長
Padding	可変長

【図4】



【図5】



【図15】

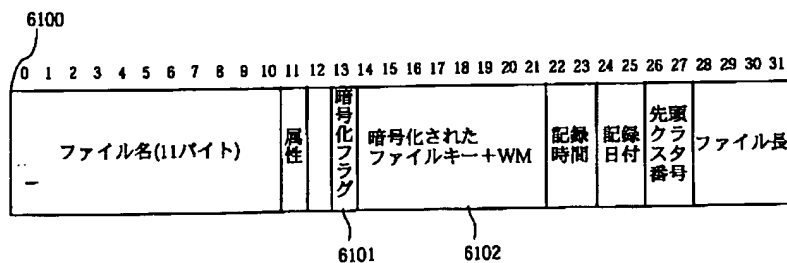
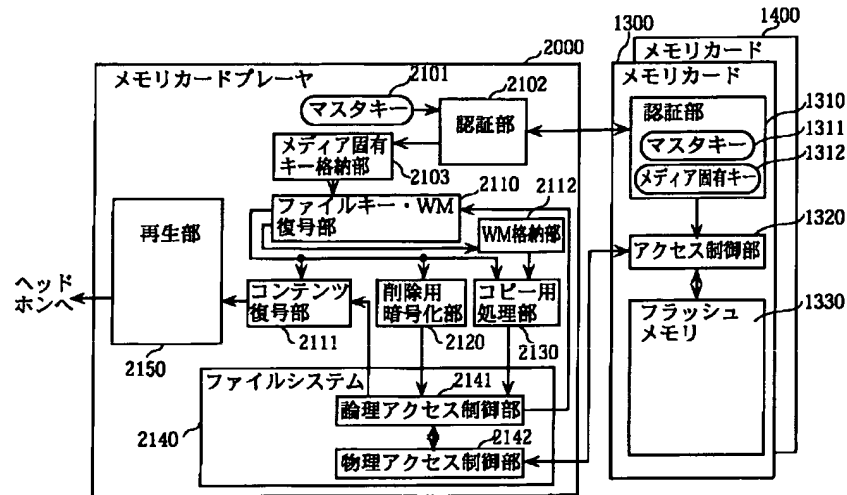


Figure 1 is a block diagram illustrating the architecture of a recording system. The diagram is divided into several main sections:

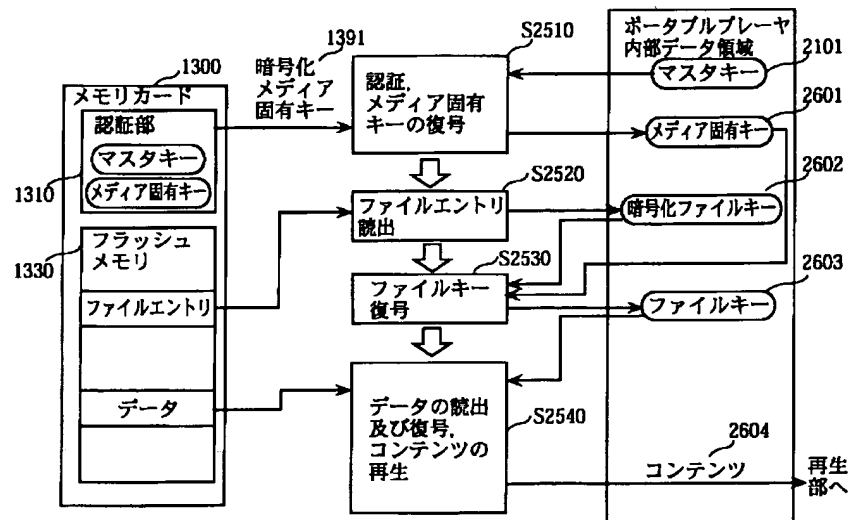
- Recording Data Domain (記録部データ領域):** Located on the left, it contains:
 - Master Key (1211):** A key used for verification and key recovery.
 - Media Inherent Key (1601):** A key derived from the Master Key.
 - File Key (1602):** A key generated from the Media Inherent Key.
 - Encrypted File Key (1603):** A key derived from the File Key.
 - Encrypted WM (1604):** A key derived from the File Key.
- Verification and Key Recovery (S1510):** A block that receives the Master Key (1211) and outputs the Media Inherent Key (1601).
- File Key Generation (S1520):** A block that receives the Media Inherent Key (1601) and outputs the File Key (1602).
- WM Extraction, File Key, and WM Encryption (S1530):** A block that receives the File Key (1602) and outputs the Encrypted File Key (1603) and Encrypted WM (1604).
- Recording (S1540):** A block that receives the Encrypted File Key (1603) and Encrypted WM (1604) and outputs the File Entry and Content.
- Memory Card (メモリカード):** Located on the right, it contains:
 - Verification Unit (1391):** Contains the Master Key and Media Inherent Key.
 - Flash Memory (1310):** Stores the File Entry and Data.
 - File Entry (1330):** Stores the File Entry.
 - Data:** Stores the Data.
- Control and Data Flow:**
 - バス情報 (Bus Information):** Represented by a line with arrows pointing to the Recording and File Key Generation blocks.
 - コンテンツ (Content):** Represented by a line with arrows pointing to the Recording and File Key Generation blocks.

Figure 1 is a perspective view of the portable device 100. The device 100 has a rectangular body. On the top surface, there is a liquid crystal display (2001) and an operation button (2002) below it. On the front face, there are two memory card insertion ports (2011 and 2012). A memory card player (2000) is located on the side of the device. A pair of headphones (2020) is connected to the side of the device. Two memory cards, 1300 and 1400, are shown being inserted into the ports 2011 and 2012 respectively.

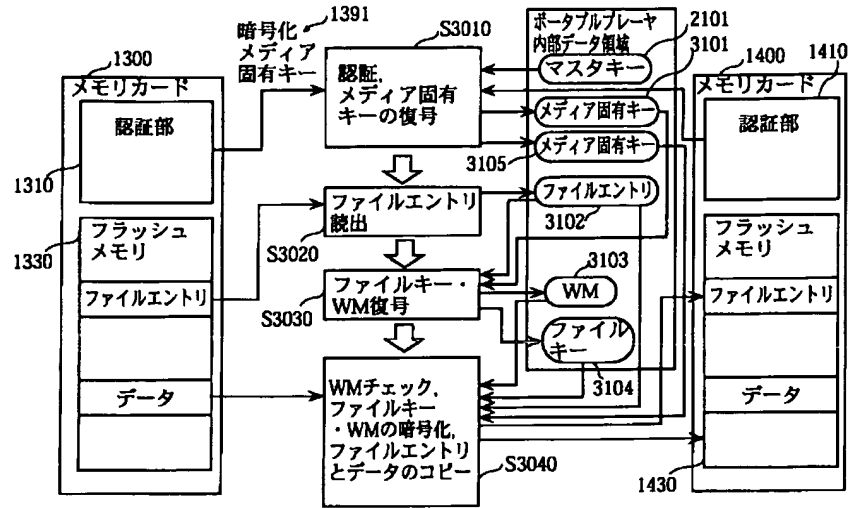
【図9】



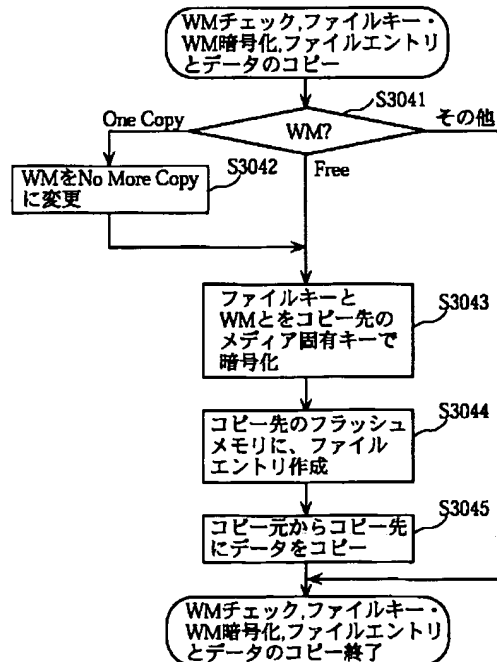
【図10】



【図11】



【図12】



フィールド名	長さ	データ
AttributeType	4	固定値:100
Attribute Sub Type	1	固定値:10
Reserved	3	0
Attribute Length	4	58
Implementation Use Length	4	20
Implementation Identifier	32	"*Flash Crypto Info"
header Checksum	2	暗号化WMまでのチェックサム
暗号化フラグ	1	80h
Reserved	1	予約00h
暗号化ファイルキー	8	暗号化データ
暗号化WM	8	暗号化データ

(51) Int. Cl.⁷

FI

G 0 6 K	17/00
	19/07
	19/073
	19/10
G 0 9 C	1/00
	5/00
G 1 1 B	20/10

660

G 0 6 K	17/00
G 0 9 C	1/00
	5/00
G 1 1 B	20/10
H 0 4 N	1/387
G 0 6 K	19/00

T 5D044
660D 5J104
H
J
P

H O 4 L 9/10
9/32
H O 4 N 1/387

H O 4 L 9/00
R
6 2 1 A
6 7 5 A

(72)発明者 館林 誠
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

Fターム(参考) 5B017 AA06 BA04 BA05 BA07 CA12
CA14 CA16
5B035 AA13 BB09 BC00 CA29 CA38
5B058 CA27 KA33 KA35 YA20
5B082 AA13 EA12 GA00 JA08
5C076 AA14 CA01
5D044 AB05 DE02 DE03 DE37 DE49
DE52 DE60 GK17 HL08 HL11
5J104 AA07 AA14 AA16 EA17 KA02
KA04 NA37 PA14